

# Sum Secrecy Rate Maximization for Full-Duplex Two-Way Relay Networks Using Alamouti-based Rank-Two Beamforming

Qiang Li, *Member, IEEE*, Wing-Kin Ma *Senior Member, IEEE*, and Dong Han

**Abstract**—Consider a two-way communication scenario where two single-antenna nodes, operating under full-duplex mode, exchange information to one another through the aid of a (full-duplex) multi-antenna relay, and there is another single-antenna node who intends to eavesdrop. The relay employs artificial noise (AN) to interfere the eavesdropper's channel, and amplify-forward (AF) Alamouti-based rank-two beamforming to establish the two-way communication links of the legitimate nodes. Our problem is to optimize the rank-two beamformer and AN covariance for sum secrecy rate maximization (SSRM). This SSRM problem is nonconvex, and we develop an efficient solution approach using semidefinite relaxation (SDR) and minorization-maximization (MM). We prove that SDR is tight for the SSRM problem and thus introduces no loss. Also, we consider an inexact MM method where an approximately but computationally cheap MM solution update is used in place of the exact update in conventional MM. We show that this inexact MM method guarantees convergence to a stationary solution to the SSRM problem. The effectiveness of our proposed approach is further demonstrated by an energy-harvesting scenario extension, and by extensive simulation results.

**Index terms**— Physical-layer security, full-duplex relay, minorization-maximization, semidefinite relaxation.

## I. INTRODUCTION

With the recent advances of self-interference cancellation techniques, full-duplex (FD) communication has received renewed interest. Particularly, FD has been seen as a promising physical-layer technology to meet the explosive data requirement for the future 5G mobile networks [1]. In contrast to frequency-division duplex (FDD) and time-division duplex (TDD), FD has the potential to double the spectral efficiency by simultaneously transmitting and receiving (STR) over the same radio-frequency (RF) bands. FD also provides new opportunities for system designs to achieve some specific goals, such as physical-layer (PHY) security [2]–[10] and simultaneous wireless information and power transfer (SWIPT) [11]–[14].

PHY security is an information theoretic approach for providing information security at the PHY layer by exploiting

the difference between the decoding abilities of the target user and eavesdropper. An effective way to deliver PHY security is to adopt the so-called artificial noise (AN) approach, where the transmitter intentionally generates noise to jam the eavesdropper. Interestingly, with FD STR transceivers, we can apply AN even more effectively. In [2], the authors exploit the full duplexity of the target user to simultaneously receive information and transmit AN. Motivated by the aforementioned work, PHY security using FD has received considerable attention. Specifically, the work [3] analyzed the secure degrees of freedom in FD point-to-point transmission. For FD two-way secure communications, robust and low-complexity transmit solutions have been developed in [4] and [5], respectively. In [6] and [7], the authors considered secrecy designs in cellular networks with an FD base station (BS) and multiple half-duplex uplink/downlink mobile users. For both of these works, the semidefinite relaxation-based approach was employed either to maximize the downlink secrecy rate [6] or to minimize the uplink/downlink transmission powers under secrecy rate constraints [7]. FD relay secure communication has also gained much interest [8]–[10]. In [8], the authors considered one-way FD secure relay networks, where two operation modes of the FD relay are considered, namely full-duplex transmission (FDT) and full-duplex jamming (FDJ). A secrecy outage probability comparison between FDT and FDJ was conducted in [9], and the result reveals that FDJ is more suitable for the small target secrecy rate regime. Extension to a multi-hop FD relay network has also been considered in [10].

Apart from PHY security, another emerging application of full duplexity is SWIPT. SWIPT is a means of using RF signals to achieve dual transmission of information and energy; readers are referred to the recent magazine paper [15] for a more complete treatment of this kind of technique. With the FD capability, a communication node can simultaneously receive information from and broadcast energy to other nodes, or do the opposite. Under this new information-energy paradigm, various resource allocations and protocol designs have been proposed. For example, the works [11], [12] considered the resource allocation problem for an information-energy hybrid cellular network, where an FD BS broadcasts energy to power users in the downlink, and at the same time each user transmits information in the uplink in a TDD manner. Optimal time and power allocations were derived in [11], [12]. In [13], [14], a two-hop relay system with an FD energy harvesting relay was studied. In particular, the work [13] proposed to split the transmission into two stages for power transfer and

Qiang Li is with School of Communication and Information Engineering, University of Electronic Science and Technology of China, Chengdu, P. R. China. E-mail: lq@uestc.edu.cn

Wing-Kin Ma is with the Department of Electronic Engineering, The Chinese University of Hong Kong, Shatin, Hong Kong S.A.R., China. E-mail: wkma@iee.org.

Dong Han is with the Department of Electrical Engineering, The University of Texas at Dallas (UTD), Richardson, TX. E-mail: dxh151130@utdallas.edu

information forwarding, and analyzed the rate performance of FD relaying under different harvesting antenna settings and transmission modes. In [14], the authors considered a different relaying protocol to allow the relay to harvest energy and forward information concurrently.

In this work, we consider exploiting full duplexity to enhance PHY security and achieve SWIPT. Specifically, we focus on FD two-way relay networks, where two legitimate nodes simultaneously transmit and receive confidential information through an FD multi-antenna relay, and an eavesdropper overhears the transmission from both the two legitimate nodes and the relay. Unlike the previous works on FD two/multi-hop relay network [9], [16], [17], where the relay operates under either FDT mode or FDJ mode, we consider a more general relaying strategy—simultaneously relaying information and sending jamming signal. In particular, an AN-aided Alamouti-based rank-two beamforming strategy [18] is employed to forward the confidential information. Our goal is to jointly optimize the rank-two beamforming matrix and the AN covariance matrix, such that the sum secrecy rate of the two-way transmission is maximized. This sum secrecy rate maximization (SSRM) problem is nonconvex by nature, but can be converted into a form suitable for minorization-maximization (MM) after applying the rank-two semidefinite relaxation (SDR) technique. Thus, the classical MM approach [19] can be invoked to iteratively compute a stationary solution to the relaxed SSRM problem. Since the stationary guarantee holds for the relaxed SSRM problem, but not directly for the original SSRM problem, we further develop a specific way to retrieve a stationary solution to the latter from any stationary solution to the former. The key idea is to exploit the rank-two beamforming structure to pin down the SDR tightness. We should point out that the classical MM approach requires solving each MM subproblem to optimality, which could be computational demanding in practice. In light of this drawback, we further propose an *inexact* MM approach to the SSRM problem, under which an approximate solution is sought at each iteration via an iteration-limited projected gradient method. We prove that the proposed inexact MM has the same stationary convergence guarantee as the classical (exact) MM.

As an extension, we further consider the above two-way FD relay secrecy design with a wireless energy-harvesting eavesdropper. In particular, we assume that the eavesdropper is also a system user who aims to harvest energy, but could potentially eavesdrop the confidential information. In such a case, the AN plays a dual role — on one hand, it jams the eavesdropper to secure the two-way communication; on the other hand, it also provides a source of energy for the eavesdropper to harvest. Our goal here is again to maximize the system's sum secrecy rate with the energy harvesting constraint on the eavesdropper. Following our SDR-based MM approach, we show that a stationary solution to the SSRM problem with energy harvesting can also be iteratively computed via either exact or inexact MM updates.

Our main contributions are summarized below:

- We studied a joint Alamouti-based rank-two beamforming and AN design for secrecy sum rate maximization

in a full-duplex two-way relay network, with direct links between the legitimate nodes and the eavesdropper. This formulation was not considered in the prior literature.

- We developed an SDR-based MM approach for the aforementioned design formulation. This proposed approach guarantees convergence to a stationary solution, and the proof technique, which connects SDR tightness and MM, is new.
- Further, we proposed an inexact alternative to the SDR-based MM approach for low-complexity implementation. We showed that this inexact MM guarantees convergence to a stationary solution.
- We considered a scenario extension where the eavesdropper is also an energy-harvesting user.

#### A. Organization and Notations

This paper is organized as follows. The system model and problem statement are given in Section II. Section III focuses on the SSRM problem and develops an SDR-based MM approach. Section IV proposes an inexact MM approach to the SSRM problem. Extension to the energy-harvesting eavesdropper case is considered in Section V. Simulation results comparing the proposed designs are illustrated in Section VI. Section VII concludes the paper.

Our notations are as follows.  $(\cdot)^T$ ,  $(\cdot)^*$  and  $(\cdot)^H$  denote transpose, conjugate and conjugate transpose, respectively;  $\mathbf{I}$  denotes an identity matrix with appropriate dimension;  $\mathbb{H}_+^N$  denotes the set of all  $N$ -by- $N$  Hermitian positive semidefinite matrices;  $\mathbf{A} \succeq \mathbf{0}$  means that  $\mathbf{A}$  is Hermitian positive semidefinite, and  $\mathbf{A} \succ \mathbf{0}$  means that  $\mathbf{A}$  is Hermitian positive definite;  $\text{Diag}(a, b)$  represents a diagonal matrix with diagonal elements  $a$  and  $b$ ;  $[\cdot]^+$  is the projection onto the set of non-negative numbers;  $\mathcal{CN}(\mathbf{a}, \mathbf{\Sigma})$  represents complex Gaussian distribution with mean  $\mathbf{a}$  and covariance matrix  $\mathbf{\Sigma}$ .

## II. SYSTEM MODEL AND PROBLEM FORMULATION

The scenario of interest is depicted in Fig. 1. Two legitimate nodes, named Alice and Bob herein, perform two-way communication with the aid of a relay. Alice, Bob and the relay are equipped with full-duplex RF transceivers, and thus they can simultaneously transmit and receive over the same RF band. Alice has one antenna for transmission and one antenna for reception, and the same applies to Bob. The relay has  $N$  antennas for transmission and  $M$  antennas for reception. The transmission is overheard by an eavesdropper, named Eve, who has one antenna. The problem is to design a transmission scheme such that the two-way messages are both secured from a PHY information security perspective.

#### A. Received Signal Model at Alice and Bob

Let us first describe the basic signal model. Alice and Bob transmit coded confidential information signals  $s_A(t) \in \mathbb{C}$  and  $s_B(t) \in \mathbb{C}$  to Bob and Alice, respectively (resp.). There is no direct link between Alice and Bob, and the information signals are forwarded by the relay. Let  $\mathbf{h}_{i,R} \in \mathbb{C}^M$ ,  $i \in \{A, B\}$ , denote the channel from node  $i$  to the receive antennas of

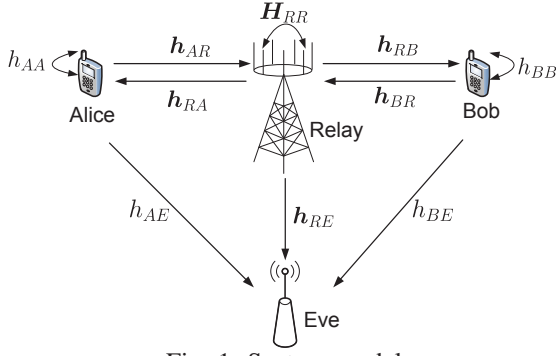


Fig. 1: System model.

the relay, where nodes  $A$  and  $B$  refer to Alice and Bob, resp. Also, let  $\mathbf{H}_{RR} \in \mathbb{C}^{M \times N}$  denote the channel from the transmit antennas to the receive antennas of the relay, i.e., the so-called self-interference (SI) channel. The relay's received signal at the  $t$ th time index is modeled as

$$\mathbf{y}_R(t) = \mathbf{h}_{AR}s_A(t) + \mathbf{h}_{BR}s_B(t) + \mathbf{H}_{RR}\mathbf{x}_R(t) + \mathbf{n}_R(t), \quad t = 1, 2, \dots \quad (1)$$

where  $\mathbf{x}_R(t) \in \mathbb{C}^N$  is the transmit signal at the relay, which aims at simultaneously forwarding the confidential information signals to Bob and Alice;  $\mathbf{n}_R(t) \sim \mathcal{CN}(\mathbf{0}, \sigma_R^2 \mathbf{I})$  is additive white Gaussian noise (AWGN). The format that  $\mathbf{x}_R(t)$  takes will be described soon. Note that the third term  $\mathbf{H}_{RR}\mathbf{x}_R(t)$  on the right-hand side (RHS) of (1) is the full-duplex SI, which has a much larger dynamic range than the signal components  $\mathbf{h}_{AR}s_A(t)$  and  $\mathbf{h}_{BR}s_B(t)$ . However, the full-duplex SI can be eliminated by applying nulling, where  $\mathbf{x}_R(t)$  is designed such that  $\mathbf{H}_{RR}\mathbf{x}_R(t) = \mathbf{0}$  [20]. We will take on this SI nulling strategy<sup>1</sup>. Moreover, the received signals at Alice and Bob are

$$y_i(t) = \mathbf{h}_{R,i}^H \mathbf{x}_R(t) + h_{i,i}s_i(t) + n_i(t), \quad i \in \{A, B\}, \quad t = 1, 2, \dots \quad (2)$$

where, for  $i \in \{A, B\}$ ,  $y_i(t)$  is the received signal at node  $i$ ;  $\mathbf{h}_{R,i} \in \mathbb{C}^N$  is the channel from the relay to node  $i$ ;  $n_i(t) \sim \mathcal{CN}(0, \sigma_i^2)$  is AWGN. Again, the second term  $h_{i,i}s_i(t)$  on the RHS of (2) is full-duplex SI. Since Alice and Bob have one receive antenna only, the aforementioned SI nulling strategy is not applicable. However, since Alice (resp. Bob) has knowledge of its own transmitted signal  $s_A(t)$  (resp.  $s_B(t)$ ), it can cancel the SI term  $h_{AA}s_A(t)$  (resp.  $h_{BB}s_B(t)$ ) from (2). Such signal cancellation is however imperfect owing to issues such as the large dynamic range of the full-duplex SI; see [1] for details. The SI-cancelled signal of  $y_i(t)$  can be modeled as

$$\bar{y}_i(t) = \mathbf{h}_{R,i}^H \mathbf{x}_R(t) + \sqrt{\kappa_i} h_{i,i} s_i(t) + n_i(t), \quad i \in \{A, B\}, \quad t = 1, 2, \dots$$

where  $0 < \kappa_i < 1$  is the full-duplex SI residual factor of node  $i$  [13].

<sup>1</sup>Implicitly, we have assumed  $N > M$  so that nulling can be done at the relay's transmission stage. On the other hand, for the case of  $N < M$ , a similar nulling process can be performed at the relay's reception stage; readers are referred to our previous abridged conference paper [21] for the latter case.

The transmission format of  $\mathbf{x}_R(t)$  is specified as follows. We consider a combination of amplify-and-forward (AF) beamforming, Alamouti space-time coding and artificial noise (AN) strategies. As mentioned previously, we assume SI nulling where the received signal in (1) is reduced to  $\mathbf{y}_R(t) = \mathbf{h}_{AR}s_A(t) + \mathbf{h}_{BR}s_B(t) + \mathbf{n}_R(t)$ . The relay first obtains soft estimates of  $s_A(t)$  and  $s_B(t)$  via the minimum mean-square-error (MMSE) reception

$$\hat{s}_i(t) = \mathbf{f}_i^H \mathbf{y}_R(t), \quad i \in \{A, B\},$$

where  $\mathbf{f}_A = (\sigma_R^2 \mathbf{I} + \sum_{i \in \{A, B\}} p_i \mathbf{h}_{iR} \mathbf{h}_{iR}^H)^{-1} \mathbf{h}_{AR}$ ;  $\mathbf{f}_B = (\sigma_R^2 \mathbf{I} + \sum_{i \in \{A, B\}} p_i \mathbf{h}_{iR} \mathbf{h}_{iR}^H)^{-1} \mathbf{h}_{BR}$ ;  $p_i = \mathbb{E}\{|s_i(t)|^2\}$ ,  $i \in \{A, B\}$ . Then, the estimates  $\hat{s}_A(t)$  and  $\hat{s}_B(t)$  are parsed into blocks via  $\hat{\mathbf{s}}_i(n) = [\hat{s}_i(2n-1) \hat{s}_i(2n)]^T$ , where  $i \in \{A, B\}$ , and  $n = 1, 2, \dots$  denotes the block index. Similarly, let  $\mathbf{X}_R(n) = [\mathbf{x}_R(2n-1) \mathbf{x}_R(2n)]$  denote the  $n$ th block of the relay's transmit signal. At every block  $n$ , the relay uses an AF-beamformed Alamouti scheme to forward the estimated information blocks  $\hat{\mathbf{s}}_A(n)$  and  $\hat{\mathbf{s}}_B(n)$ . To be specific, we have

$$\mathbf{X}_R(n) = \mathbf{W}_0 \mathbf{C}(\hat{\mathbf{s}}_A(n) + \hat{\mathbf{s}}_B(n)) + \mathbf{Z}(n), \quad (3)$$

where  $\mathbf{W}_0 \in \mathbb{C}^{N \times 2}$  is a transmit beamforming matrix;

$$\mathbf{C}(\mathbf{s}) = \begin{bmatrix} s_1 & s_2^* \\ s_2 & -s_1^* \end{bmatrix}$$

is the Alamouti space-time code;  $\mathbf{Z}(n) = [\mathbf{z}(2n-1) \mathbf{z}(2n)] \in \mathbb{C}^{N \times 2}$  is a superimposed AN for jamming Eve, in which  $\mathbf{z}(t)$  follows an i.i.d. complex Gaussian distribution with mean zero and covariance  $\mathbf{Q}_0 \in \mathbb{H}_+^N$ . To fulfill the SI nulling condition  $\mathbf{H}_{RR}\mathbf{x}_R(n) = \mathbf{0}$ ,  $\mathbf{W}_0$  and  $\mathbf{Q}_0$  are restricted to satisfy  $\mathbf{H}_{RR}\mathbf{W}_0 = \mathbf{0}$  and  $\mathbf{H}_{RR}\mathbf{Q}_0 = \mathbf{0}$ , resp. Let us examine the corresponding received signals at Alice and Bob. By letting  $\bar{\mathbf{y}}_i(n) = [\bar{y}_i(2n-1) \bar{y}_i(2n)]$ ,  $\mathbf{s}_i(n) = [s_i(2n-1) s_i(2n)]$ ,  $i \in \{A, B\}$ , we have

$$\bar{\mathbf{y}}_i(n) = \mathbf{h}_{R,i}^H \mathbf{W}_0 \mathbf{C}(\hat{\mathbf{s}}_B(n)) + \mathbf{h}_{R,i}^H \mathbf{W}_0 \mathbf{C}(\hat{\mathbf{s}}_A(n)) + \mathbf{h}_{R,i}^H \mathbf{Z}(n) + \sqrt{\kappa_i} h_{i,i} s_i(n+1) + \mathbf{n}_i(n). \quad (4)$$

Suppose  $i = A$ . Then, the terms involving  $s_A(2n-1)$  and  $s_A(2n)$  in the above equation is the AF-induced self-interference, and it can be eliminated by direct cancellation [22]. Subsequently, by applying the standard Alamouti reception [23] to the SI-cancelled version of  $\bar{\mathbf{y}}_A(n)$ , it can be verified that the elements of  $\mathbf{s}_B(n)$  can be decoupled from  $\bar{\mathbf{y}}_A(n)$  with the same signal-to-interference-plus-noise ratio (SINR). Particularly, it can be shown from the above system setup that the SINR of  $\mathbf{s}_B(n)$  at Alice is

$$\text{SINR}_A(\mathbf{W}_0, \mathbf{Q}_0) = \frac{\tilde{p}_B \|\mathbf{h}_{RA}^H \mathbf{W}_0\|^2}{\tilde{\sigma}_R^2 \|\mathbf{h}_{RA}^H \mathbf{W}_0\|^2 + \mathbf{h}_{RA}^H \mathbf{Q}_0 \mathbf{h}_{RA} + \tilde{\sigma}_A^2},$$

where  $\tilde{p}_B \triangleq p_B |(\mathbf{f}_A + \mathbf{f}_B)^H \mathbf{h}_{BR}|^2$ ,  $\tilde{\sigma}_R^2 \triangleq \sigma_R^2 \|\mathbf{f}_A + \mathbf{f}_B\|^2$ ,  $\tilde{\sigma}_A^2 \triangleq \sigma_A^2 + \kappa_A p_A |h_{AA}|^2$ . Also, the above argument applies to  $i = B$ , and the SINR of  $\mathbf{s}_A(t)$  at Bob is

$$\text{SINR}_B(\mathbf{W}_0, \mathbf{Q}_0) = \frac{\tilde{p}_A \|\mathbf{h}_{RB}^H \mathbf{W}_0\|^2}{\tilde{\sigma}_R^2 \|\mathbf{h}_{RB}^H \mathbf{W}_0\|^2 + \mathbf{h}_{RB}^H \mathbf{Q}_0 \mathbf{h}_{RB} + \tilde{\sigma}_B^2},$$

where  $\tilde{p}_A \triangleq p_A |(\mathbf{f}_A + \mathbf{f}_B)^H \mathbf{h}_{AR}|^2$ ,  $\tilde{\sigma}_B^2 \triangleq \sigma_B^2 + \kappa_B p_B |h_{BB}|^2$ .



### B. Received Signal Model at Eve

Let us consider the received signal model at Eve under the aforementioned system setup. Eve's received signal is modeled as

$$y_E(t) = \mathbf{h}_{RE}^H \mathbf{x}_R(t) + h_{AE}s_A(t) + h_{BE}s_B(t) + n_E(t), \quad (5)$$

$$t = 1, 2, \dots$$

where  $\mathbf{h}_{RE} \in \mathbb{C}^N$  is the channel from the relay to Eve;  $h_{i,E} \in \mathbb{C}$ ,  $i \in \{A, B\}$ , is the channel from node  $i$  to Eve;  $n_E(t) \sim \mathcal{CN}(0, \sigma_E^2)$  is noise. Note that in the above model, there are direct links between the legitimate nodes and Eve. Denote  $\mathbf{y}_E(n) = [y_E(2n-1) \ y_E(2n)]$ . Similar to (4), it can be shown that

$$\mathbf{y}_E(n) = \mathbf{h}_{RE}^H \mathbf{W}_0 \mathbf{C}(\hat{\mathbf{s}}_B(n)) + \mathbf{h}_{RE}^H \mathbf{W}_0 \mathbf{C}(\hat{\mathbf{s}}_A(n)) + \mathbf{h}_{RE}^H \mathbf{Z}(n) + \sum_{i \in \{A, B\}} h_{i,E} \mathbf{s}_i(n+1) + \mathbf{n}_E(n). \quad (6)$$

From the above formula, we observe that  $\mathbf{s}_A(n)$  and  $\mathbf{s}_B(n)$  are present in both  $\mathbf{y}_E(n)$  and  $\mathbf{y}_E(n-1)$ . Let us assume that Eve intends to decode  $\mathbf{s}_A(n)$  and  $\mathbf{s}_B(n)$  from  $\mathbf{y}_E(n)$  and  $\mathbf{y}_E(n-1)$ , seeing other terms as interference and noise. Then, through some tedious derivations which are shown in Appendix A, Eve's reception can be equivalently expressed as an MIMO system

$$\tilde{\mathbf{y}}_E(t) = \mathbf{H}_E \begin{bmatrix} s_A(t) \\ s_B(t) \end{bmatrix} + \tilde{\mathbf{n}}_E(t) \in \mathbb{C}^2, \quad t = 1, 2, \dots \quad (7)$$

Here,

$$\mathbf{H}_E = \begin{bmatrix} \|\mathbf{h}_{RE}^H \mathbf{W}_0\| \tilde{f}_{AR} & \|\mathbf{h}_{RE}^H \mathbf{W}_0\| \tilde{f}_{BR} \\ h_{AE} & h_{BE} \end{bmatrix}$$

is the equivalent MIMO channel, where  $\tilde{f}_{iR} = (\mathbf{f}_A + \mathbf{f}_B)^H \mathbf{h}_{iR}$ ,  $i \in \{A, B\}$ ;  $\tilde{\mathbf{n}}_E(t)$  is the interference-plus-noise term with mean zero and covariance

$$\mathbf{\Psi} = \begin{bmatrix} \Psi_{11} & 0 \\ 0 & \Psi_{22} \end{bmatrix} \in \mathbb{R}^{2 \times 2}, \quad (8)$$

where  $\Psi_{11} = \tilde{\sigma}_R^2 \|\mathbf{h}_{RE}^H \mathbf{W}_0\|^2 + \mathbf{h}_{RE}^H \mathbf{Q}_0 \mathbf{h}_{RE} + \sigma_E^2 + \sum_{i \in \{A, B\}} p_i |h_{iE}|^2$  and  $\Psi_{22} = \mathbf{h}_{RE}^H \mathbf{Q}_0 \mathbf{h}_{RE} + \sigma_E^2 + (\tilde{p}_A + \tilde{p}_B + \tilde{\sigma}_R^2) \|\mathbf{h}_{RE}^H \mathbf{W}_0\|^2$ .

### C. Sum Secrecy Rate Maximization Problem

Under the system setup in the last two subsections, the problem is to design the AF beamforming matrix  $\mathbf{W}_0$  and the AN covariance  $\mathbf{Q}_0$  such that the sum secrecy rate of Alice and Bob is maximized under a total transmission power constraint at the relay. The secrecy achievable rate formulation is as follows. The achievable rates at Alice and Bob are modeled as

$$R_i(\mathbf{W}_0, \mathbf{Q}_0) = \log(1 + \text{SINR}_i(\mathbf{W}_0, \mathbf{Q}_0)), \quad i \in \{A, B\}, \quad (9)$$

where we treat the full-duplex residual SI as Gaussian noise; see [13], [20] for similar treatments. Also, by applying the MIMO multiple-access channel capacity result to (7), the sum achievable rate at Eve is formulated as

$$R_E(\mathbf{W}_0, \mathbf{Q}_0) = \log |\mathbf{I} + \mathbf{H}_E \mathbf{P} \mathbf{H}_E^H \mathbf{\Psi}^{-1}|, \quad (10)$$

where  $\mathbf{P} = \text{Diag}(p_A, p_B)$ . The above achievable rate can be reduced to

$$R_E(\mathbf{W}_0, \mathbf{Q}_0) = \log \left( \frac{\Psi_{22}^2 + \theta_1(\Psi_{22} + \Psi_{11}) + \theta_2 \|\mathbf{h}_{RE}^H \mathbf{W}_0\|^2}{\Psi_{11} \Psi_{22}} \right) \quad (11)$$

where  $\theta_1 = \sum_{i \in \{A, B\}} p_i |h_{iE}|^2$ ,  $\theta_2 = (\sum_{i \in \{A, B\}} p_i |\tilde{f}_{iR}|^2) \theta_1 - |\sum_{i \in \{A, B\}} \tilde{f}_{iR}^* h_{iE}|^2$ ; see Appendix B for details. From (11) and (9), we characterize the sum secrecy rate as [24]<sup>2</sup>

$$R_s(\mathbf{W}_0, \mathbf{Q}_0) \triangleq R_A(\mathbf{W}_0, \mathbf{Q}_0) + R_B(\mathbf{W}_0, \mathbf{Q}_0) - R_E(\mathbf{W}_0, \mathbf{Q}_0).$$

Moreover, from the system setup in the last subsection, it can be verified that the total transmission power at the relay is

$$p_R(\mathbf{W}_0, \mathbf{Q}_0) = \frac{1}{2} \text{Tr}(\mathbb{E}\{\mathbf{X}_R(n) \mathbf{X}_R(n)^H\}) = \zeta \text{Tr}(\mathbf{W}_0 \mathbf{W}_0^H) + \text{Tr}(\mathbf{Q}_0),$$

where  $\zeta = p_A |(\mathbf{f}_A + \mathbf{f}_B)^H \mathbf{h}_{AR}|^2 + p_B |(\mathbf{f}_A + \mathbf{f}_B)^H \mathbf{h}_{BR}|^2 + \sigma_R^2 \|\mathbf{f}_A + \mathbf{f}_B\|^2$ . The design problem is therefore formulated as follows:

$$\max_{\mathbf{Q}_0 \succeq \mathbf{0}, \mathbf{W}_0 \in \mathbb{C}^{N \times 2}} R_s(\mathbf{W}_0, \mathbf{Q}_0) \quad (12a)$$

$$\text{s.t. } p_R(\mathbf{W}_0, \mathbf{Q}_0) \leq P_R, \quad (12b)$$

$$\mathbf{H}_{RR} \mathbf{W}_0 = \mathbf{0}, \mathbf{H}_{RR} \mathbf{Q}_0 = \mathbf{0}, \quad (12c)$$

where  $P_R > 0$  is the maximal transmission power threshold at the relay, and recall that (12c) is for fulfilling the full-duplex SI nulling condition. Problem (12) will be called the *sum secrecy rate maximization* (SSRM) problem in the sequel.

### III. AN SDR-BASED MM APPROACH TO THE SSRM PROBLEM

The SSRM problem in (12) is nonconvex, and our aim is to develop an SDR-based minorization-maximization (MM) approach that will be shown to guarantee convergence to a stationary solution to problem (12). In the first subsection, we give a detailed description of our proposed approach, and in the second subsection we show the convergence of the SDR-based MM algorithm.

#### A. Description of the SDR-based MM Algorithm

Our development is as follows. First, we consider an alternative formulation of problem (12). Let  $r = \text{rank}(\mathbf{H}_{RR})$  and  $\mathbf{V}_0 \in \mathbb{C}^{N \times (N-r)}$  be the right singular vectors associated with the zero singular values of  $\mathbf{H}_{RR}$ . From (12c), it is easy to verify that any feasible point  $(\mathbf{W}_0, \mathbf{Q}_0)$  of problem (12) can be equivalently expressed as

$$\mathbf{W}_0 = \mathbf{V}_0 \tilde{\mathbf{W}}, \quad \mathbf{Q}_0 = \mathbf{V}_0 \mathbf{Q} \mathbf{V}_0^H,$$

for some  $\tilde{\mathbf{W}} \in \mathbb{C}^{(N-r) \times 2}$  and  $\mathbf{Q} \in \mathbb{H}_+^{n-r}$ . By applying the above equivalence to problem (12), and letting  $\tilde{\mathbf{W}} = \zeta^{-1/2} \mathbf{W}$ , we can rewrite problem (12) as

$$\max_{\mathbf{Q} \in \mathbb{H}_+^{n-r}, \mathbf{W} \in \mathbb{C}^{(N-r) \times 2}} \phi(\mathbf{W} \mathbf{W}^H, \mathbf{Q}) \quad (13)$$

$$\text{s.t. } \text{Tr}(\mathbf{W} \mathbf{W}^H) + \text{Tr}(\mathbf{Q}) \leq P_R,$$

<sup>2</sup>The sum secrecy rate  $R_s$  implicitly assumes that Alice and Bob can coordinately allocate their transmission rates. This can be made possible by asking the relay to coordinate the rate allocation.

$$\begin{aligned}
f(\mathbf{W}\mathbf{W}^H, \mathbf{Q}) &= \sum_{i=1}^2 \log(c_i + \alpha_i(\mathbf{W}\mathbf{W}^H, \mathbf{Q})) + \log(\psi_1(\mathbf{W}\mathbf{W}^H, \mathbf{Q})) + \log(\psi_2(\mathbf{W}\mathbf{W}^H, \mathbf{Q})), \\
g_1(\mathbf{W}\mathbf{W}^H, \mathbf{Q}) &= \sum_{i=1}^2 \log(c_i + \beta_i(\mathbf{W}\mathbf{W}^H, \mathbf{Q})), \\
g_2(\mathbf{W}\mathbf{W}^H, \mathbf{Q}) &= \log\left([\psi_2(\mathbf{W}\mathbf{W}^H, \mathbf{Q})]^2 + \theta_1[\psi_1(\mathbf{W}\mathbf{W}^H, \mathbf{Q}) + \psi_2(\mathbf{W}\mathbf{W}^H, \mathbf{Q})] + \zeta^{-1}\theta_2\text{Tr}(\mathbf{W}\mathbf{W}^H \mathbf{V}_0^H \mathbf{h}_{RE} \mathbf{h}_{RE}^H \mathbf{V}_0)\right), \\
\alpha_1(\mathbf{W}\mathbf{W}^H, \mathbf{Q}) &= \beta_1(\mathbf{W}\mathbf{W}^H, \mathbf{Q}) + \zeta^{-1}\tilde{p}_B\text{Tr}(\mathbf{W}\mathbf{W}^H \mathbf{V}_0^H \mathbf{h}_{RA} \mathbf{h}_{RA}^H \mathbf{V}_0), \\
\alpha_2(\mathbf{W}\mathbf{W}^H, \mathbf{Q}) &= \beta_2(\mathbf{W}\mathbf{W}^H, \mathbf{Q}) + \zeta^{-1}\tilde{p}_A\text{Tr}(\mathbf{W}\mathbf{W}^H \mathbf{V}_0^H \mathbf{h}_{RB} \mathbf{h}_{RB}^H \mathbf{V}_0), \\
\beta_1(\mathbf{W}\mathbf{W}^H, \mathbf{Q}) &= \zeta^{-1}\tilde{\sigma}_R^2\text{Tr}(\mathbf{W}\mathbf{W}^H \mathbf{V}_0^H \mathbf{h}_{RA} \mathbf{h}_{RA}^H \mathbf{V}_0) + \text{Tr}(\mathbf{Q}\mathbf{V}_0^H \mathbf{h}_{RA} \mathbf{h}_{RA}^H \mathbf{V}_0), \\
\beta_2(\mathbf{W}\mathbf{W}^H, \mathbf{Q}) &= \zeta^{-1}\tilde{\sigma}_R^2\text{Tr}(\mathbf{W}\mathbf{W}^H \mathbf{V}_0^H \mathbf{h}_{RB} \mathbf{h}_{RB}^H \mathbf{V}_0) + \text{Tr}(\mathbf{Q}\mathbf{V}_0^H \mathbf{h}_{RB} \mathbf{h}_{RB}^H \mathbf{V}_0), \\
\psi_1(\mathbf{W}\mathbf{W}^H, \mathbf{Q}) &= \tilde{\sigma}_R^2\zeta^{-1}\text{Tr}(\mathbf{W}\mathbf{W}^H \mathbf{V}_0^H \mathbf{h}_{RE} \mathbf{h}_{RE}^H \mathbf{V}_0) + \text{Tr}(\mathbf{Q}\mathbf{V}_0^H \mathbf{h}_{RE} \mathbf{h}_{RE}^H \mathbf{V}_0) + \sigma_E^2 + \sum_{i \in \{A, B\}} p_i |h_{iE}|^2, \\
\psi_2(\mathbf{W}\mathbf{W}^H, \mathbf{Q}) &= \text{Tr}(\mathbf{Q}\mathbf{V}_0^H \mathbf{h}_{RE} \mathbf{h}_{RE}^H \mathbf{V}_0) + \sigma_E^2 + \text{Tr}(\mathbf{W}\mathbf{W}^H \mathbf{V}_0^H \mathbf{h}_{RE} \mathbf{h}_{RE}^H \mathbf{V}_0), \\
c_1 &= \tilde{\sigma}_A^2, \quad c_2 = \tilde{\sigma}_B^2, \quad \zeta = p_A |(\mathbf{f}_A + \mathbf{f}_B)^H \mathbf{h}_{AR}|^2 + p_B |(\mathbf{f}_A + \mathbf{f}_B)^H \mathbf{h}_{BR}|^2 + \sigma_R^2 \|\mathbf{f}_A + \mathbf{f}_B\|^2.
\end{aligned} \tag{14}$$

where  $\phi(\mathbf{W}\mathbf{W}^H, \mathbf{Q}) \triangleq f(\mathbf{W}\mathbf{W}^H, \mathbf{Q}) - g_1(\mathbf{W}\mathbf{W}^H, \mathbf{Q}) - g_2(\mathbf{W}\mathbf{W}^H, \mathbf{Q})$ , and  $f$ ,  $g_1$  and  $g_2$  are defined in (14) on the top of the next page. Also, it is immediate that the solutions of problems (12) and (13) are related through  $\mathbf{W}_0 = \zeta^{1/2} \mathbf{V}_0 \mathbf{W}$  and  $\mathbf{Q}_0 = \mathbf{V}_0 \mathbf{Q} \mathbf{V}_0^H$ .

Second, we apply semidefinite relaxation (SDR) [25] to problem (13). Specifically, by noticing the following equivalence

$$\mathbf{W} = \mathbf{W}\mathbf{W}^H \iff \mathbf{W} \succeq \mathbf{0}, \text{rank}(\mathbf{W}) \leq 2,$$

we replace  $\mathbf{W}\mathbf{W}^H$  in problem (13) with  $\mathbf{W}$  and drop the nonconvex rank-two constraint on  $\mathbf{W}$  to get an SDR of problem (13) as follows:

$$\max_{\mathbf{W} \succeq \mathbf{0}, \mathbf{Q} \succeq \mathbf{0}} \phi(\mathbf{W}, \mathbf{Q}) \triangleq f(\mathbf{W}, \mathbf{Q}) - g_1(\mathbf{W}, \mathbf{Q}) - g_2(\mathbf{W}, \mathbf{Q}) \tag{15a}$$

$$\text{s.t. } \text{Tr}(\mathbf{W}) + \text{Tr}(\mathbf{Q}) \leq P_R. \tag{15b}$$

Notice that  $f(\mathbf{W}, \mathbf{Q})$  and  $g_1(\mathbf{W}, \mathbf{Q})$  are both concave with respect to (w.r.t.)  $(\mathbf{W}, \mathbf{Q})$ , whereas  $g_2(\mathbf{W}, \mathbf{Q})$  is neither convex nor concave w.r.t.  $(\mathbf{W}, \mathbf{Q})$ . Hence, problem (15) is still a nonconvex optimization problem. In the sequel, we develop an MM approach to (15) by finding a tight concave lower bound on  $\phi(\mathbf{W}, \mathbf{Q})$ .

First of all, given any feasible point  $(\hat{\mathbf{W}}, \hat{\mathbf{Q}})$  of (15), an upper bound on  $g_1(\mathbf{W}, \mathbf{Q})$  can be easily obtained from the first-order condition, or linearization of  $g_1$  at  $(\hat{\mathbf{W}}, \hat{\mathbf{Q}})$ , i.e.,

$$g_1(\mathbf{W}, \mathbf{Q}) \leq \tilde{g}_1(\mathbf{W}, \mathbf{Q}; \hat{\mathbf{W}}, \hat{\mathbf{Q}}),$$

where  $\tilde{g}_1(\mathbf{W}, \mathbf{Q}; \hat{\mathbf{W}}, \hat{\mathbf{Q}}) \triangleq g_1(\hat{\mathbf{W}}, \hat{\mathbf{Q}}) + \text{Tr}(\nabla_{\mathbf{W}} g_1(\hat{\mathbf{W}}, \hat{\mathbf{Q}})^H (\mathbf{W} - \hat{\mathbf{W}})) + \text{Tr}(\nabla_{\mathbf{Q}} g_1(\hat{\mathbf{W}}, \hat{\mathbf{Q}})^H (\mathbf{Q} - \hat{\mathbf{Q}}))$ . For  $g_2(\mathbf{W}, \mathbf{Q})$ , we make use of the inequality  $\log(x) \leq \log(\hat{x}) + \frac{x - \hat{x}}{\hat{x}}$  to obtain

$$g_2(\mathbf{W}, \mathbf{Q}) \leq \tilde{g}_2(\mathbf{W}, \mathbf{Q}; \hat{\mathbf{W}}, \hat{\mathbf{Q}}),$$

where

$$\begin{aligned}
\tilde{g}_2(\mathbf{W}, \mathbf{Q}; \hat{\mathbf{W}}, \hat{\mathbf{Q}}) &\triangleq g_2(\hat{\mathbf{W}}, \hat{\mathbf{Q}}) - 1 + \\
&\frac{(\psi_2)^2 + \theta_1(\psi_1 + \psi_2) + \theta_2\zeta^{-1}\mathbf{h}_{RE}^H \mathbf{V}_0 \mathbf{W} \mathbf{V}_0^H \mathbf{h}_{RE}}{(\hat{\psi}_2)^2 + \theta_1(\hat{\psi}_1 + \hat{\psi}_2) + \theta_2\zeta^{-1}\mathbf{h}_{RE}^H \mathbf{V}_0 \hat{\mathbf{W}} \mathbf{V}_0^H \mathbf{h}_{RE}},
\end{aligned}$$

and for notational simplicity we have dropped the arguments of  $\psi_i$  and used  $\hat{\psi}_i$  to represent  $\psi_i(\hat{\mathbf{W}}, \hat{\mathbf{Q}})$ .

Now, the proposed MM algorithm recursively solves the following optimization problem

$$(\mathbf{W}^{k+1}, \mathbf{Q}^{k+1}) \in \underset{\mathbf{W} \succeq \mathbf{0}, \mathbf{Q} \succeq \mathbf{0}}{\text{argmax}} \tilde{\phi}(\mathbf{W}, \mathbf{Q}; \mathbf{W}^k, \mathbf{Q}^k) \tag{16a}$$

$$\text{s.t. } \text{Tr}(\mathbf{W}) + \text{Tr}(\mathbf{Q}) \leq P_R, \tag{16b}$$

until some stopping rule is met. In (16), we have defined  $\tilde{\phi}(\mathbf{W}, \mathbf{Q}; \mathbf{W}^k, \mathbf{Q}^k) \triangleq f(\mathbf{W}, \mathbf{Q}) - \tilde{g}_1(\mathbf{W}, \mathbf{Q}; \mathbf{W}^k, \mathbf{Q}^k) - \tilde{g}_2(\mathbf{W}, \mathbf{Q}; \mathbf{W}^k, \mathbf{Q}^k)$  for  $k = 0, 1, \dots$  and some feasible starting point  $(\mathbf{W}^0, \mathbf{Q}^0)$ .

Problem (16) is a convex problem, which can be optimally solved, e.g., by CVX [26]. Moreover, by direct application of the MM convergence result [27, Theorem 1], we conclude that every limit point of  $\{(\mathbf{W}^k, \mathbf{Q}^k)\}_k$  is a stationary solution to problem (15).

The MM approach proposed above is, at first look, an MM approach to the relaxed SSRM problem in (15), rather than the original SSRM problem. Thus, it is important to understand whether problem (15) can provide a tight relaxation to the original SSRM problem (13), and whether we can obtain a stationary solution to the original SSRM problem from the proposed MM iteration. We address these issues in the next subsection.

## B. SDR Tightness and Stationary Convergence

In this subsection, we establish the SDR tightness and the stationary convergence of the MM iteration. Since problem (16) has a compact feasible set, the iterate  $\{(\mathbf{W}^k, \mathbf{Q}^k)\}_k$  generated by the MM iteration in (16) has at least one limit point. Suppose that  $(\bar{\mathbf{W}}, \bar{\mathbf{Q}})$  is any limit point of  $\{(\mathbf{W}^k, \mathbf{Q}^k)\}_k$ . Consider the following two problems:

$$\begin{aligned}
&\max_{\mathbf{W} \succeq \mathbf{0}, \mathbf{Q} \succeq \mathbf{0}} \tilde{\phi}(\mathbf{W}, \mathbf{Q}; \bar{\mathbf{W}}, \bar{\mathbf{Q}}) \\
&\text{s.t. } \text{Tr}(\mathbf{W}) + \text{Tr}(\mathbf{Q}) \leq P_R,
\end{aligned} \tag{17}$$

and

$$\min_{\mathbf{W} \succeq \mathbf{0}, \mathbf{Q} \succeq \mathbf{0}} \text{Tr}(\mathbf{W}) + \text{Tr}(\mathbf{Q}) \quad (18a)$$

$$\text{s.t. } \alpha_i(\mathbf{W}, \mathbf{Q}) = \alpha_i(\bar{\mathbf{W}}, \bar{\mathbf{Q}}), \quad i = 1, 2, \quad (18b)$$

$$\beta_i(\mathbf{W}, \mathbf{Q}) = \beta_i(\bar{\mathbf{W}}, \bar{\mathbf{Q}}), \quad i = 1, 2, \quad (18c)$$

$$\psi_i(\mathbf{W}, \mathbf{Q}) = \psi_i(\bar{\mathbf{W}}, \bar{\mathbf{Q}}), \quad i = 1, 2, \quad (18d)$$

$$\text{Tr}(\mathbf{W}\mathbf{V}_0^H \mathbf{h}_{RE} \mathbf{h}_{RE}^H \mathbf{V}_0) = \text{Tr}(\bar{\mathbf{W}}\mathbf{V}_0^H \mathbf{h}_{RE} \mathbf{h}_{RE}^H \mathbf{V}_0), \quad (18e)$$

where  $\alpha_i$ ,  $\beta_i$  and  $\tilde{\phi}$  are defined in (14) and (16a), resp. Problems (17) and (18) are closely related, as revealed by the following lemma.

**Lemma 1** *Let  $(\mathbf{W}^*, \mathbf{Q}^*)$  be any optimal solution to problem (18). Then,  $(\mathbf{W}^*, \mathbf{Q}^*)$  is also an optimal solution to problem (17).*

The proof of Lemma 1 is relegated to Appendix C. Using Lemma 1, we establish the following main result:

**Theorem 1** *There exists an optimal solution  $(\mathbf{W}^*, \mathbf{Q}^*)$  to problem (17) such that  $\text{rank}(\mathbf{W}^*) \leq 2$ ; i.e.,  $\mathbf{W}^*$  can be decomposed as  $\mathbf{W}^* \mathbf{W}^{*H}$  for some  $\mathbf{W}^* \in \mathbb{C}^{(N-r) \times 2}$ . Moreover,  $(\mathbf{W}^*, \mathbf{Q}^*)$  is a stationary solution or Karush-Kuhn-Tucker (KKT) solution to problem (13).*

The proof of Theorem 1 is shown in Appendix D. The idea behind the proof is to use the semidefinite program (SDP) rank-reduction result [28] to show the existence of a rank-two optimal  $\mathbf{W}^*$  for problem (17). Theorem 1 not only pins down the SDR tightness, it also gives a procedure of recovering a stationary solution to the SSRM problem (13). Specifically, after the convergence of the MM iteration, if  $\mathbf{W}$  has rank no greater than two, we can simply obtain a stationary solution to problem (13) by applying square-root (and rank-two) decomposition to  $\bar{\mathbf{W}}$ ; otherwise, we form the problem in (18) and apply the rank-reduction procedure to obtain a rank-two beamforming solution to problem (13) with stationarity guarantee. We should mention that the rank-reduction procedure can be efficiently performed (with polynomial-time complexity); readers are referred to [28] for details.

To summarize, we have developed an MM approach for computing a stationary solution to the SSRM problem (13) iteratively. However, as one may have noticed, each MM iteration in (16) requires solving a convex optimization problem to optimality, which could be computationally demanding. In view of this drawback, in the next section we will propose a low-complexity MM alternative via inexact MM updates.

#### IV. AN INEXACT MM APPROACH TO THE SSRM PROBLEM (12)

In this section, we present an inexact MM algorithm for the SSRM problem. In addition to computational efficiency, the inexact MM algorithm to be presented is guaranteed to converge to a stationary solution to the SSRM problem.

##### A. A General Inexact MM Framework

Let us first introduce the notion of *gradient mapping* [29], which will be useful for characterizing the solution inexactness and stationarity of the method to be considered. Consider an optimization problem

$$\begin{aligned} \max_{\mathbf{x}} \quad & \varphi(\mathbf{x}) \\ \text{s.t.} \quad & \mathbf{x} \in \mathcal{C}. \end{aligned} \quad (19)$$

where the objective function  $\varphi(\mathbf{x})$  is continuously differentiable (not necessarily convex), and the feasible set  $\mathcal{C}$  is convex and compact. The gradient mapping of  $\varphi(\mathbf{x})$  at  $\bar{\mathbf{x}} \in \mathcal{C}$  is defined as

$$\tilde{\nabla}\varphi(\bar{\mathbf{x}}) \triangleq \mathcal{P}(\bar{\mathbf{x}} + \nabla\varphi(\bar{\mathbf{x}})) - \bar{\mathbf{x}}, \quad (20)$$

where  $\mathcal{P}(\mathbf{x})$  represents the projection of  $\mathbf{x}$  on  $\mathcal{C}$ . The following result characterizes the relationship between gradient mapping and stationarity:

**Lemma 2 ([30])** *A point  $\bar{\mathbf{x}} \in \mathcal{C}$  is a stationary solution to problem (19) if and only if  $\tilde{\nabla}\varphi(\bar{\mathbf{x}}) = \mathbf{0}$ .*

Now, let us turn back to the MM subproblem (16), which is restated below:

$$\begin{aligned} \max_{\mathbf{x}} \quad & \tilde{\phi}(\mathbf{x}; \mathbf{x}^k) \\ \text{s.t.} \quad & \mathbf{x} \in \mathcal{D}, \end{aligned} \quad (21)$$

where, for notational convenience, we denote  $\mathbf{x} \triangleq (\mathbf{W}, \mathbf{Q})$  and  $\mathcal{D} \triangleq \{(\mathbf{W}, \mathbf{Q}) \mid \text{Tr}(\mathbf{W} + \mathbf{Q}) \leq P_R, \mathbf{W} \succeq \mathbf{0}, \mathbf{Q} \succeq \mathbf{0}\}$ . Instead of solving problem (21) exactly, we perform an update via the following rule:

Find a point  $\mathbf{x}^{k+1} \in \mathcal{D}$  such that

$$\tilde{\phi}(\mathbf{x}^{k+1}; \mathbf{x}^k) - \tilde{\phi}(\mathbf{x}^k; \mathbf{x}^k) \geq \zeta^k \|\tilde{\nabla}\tilde{\phi}(\mathbf{x}^k; \mathbf{x}^k)\|^2, \quad (22)$$

where  $\zeta^k > 0$  is an iteration-dependent constant and is bounded away from zero.

We call (22) an inexact updating rule; the reason is that the exact MM update (or the optimal solution to problem (21)) satisfies (22), but the converse is not true. We will specify in the next subsection how we build an efficient update that satisfies (22). For now, let us focus on the guarantee of convergence to a stationary solution. We have the following result:

**Proposition 1** *Suppose that  $\{\mathbf{x}^k\}$  is a sequence generated by an inexact updating rule in (22). Then, every limit point of  $\{\mathbf{x}^k\}$  is a stationary solution to problem (15).*

The key of the proof of Proposition 1 is that the updating rule (22) ensures sufficient improvement between the consecutive iterations if the current point is not stationary. By accumulating these improvements, the inexact MM iteration will finally reside at a stationary solution. The detailed proof is given in Appendix E. In light of Proposition 1, a result similar to Theorem 1 is established as follows.

**Theorem 2** *Let  $\hat{\mathbf{x}} = (\hat{\mathbf{W}}, \hat{\mathbf{Q}})$  be any limit point generated by an inexact MM rule in (22), and consider the problems (17)*

and (18) with  $(\bar{\mathbf{W}}, \bar{\mathbf{Q}})$  replaced by  $(\hat{\mathbf{W}}, \hat{\mathbf{Q}})$ . Then, it holds true that there exists an optimal solution  $(\mathbf{W}^*, \mathbf{Q}^*)$  to problem (17) such that  $\mathbf{W}^* = \mathbf{W}^* \mathbf{W}^{*H}$  for some  $\mathbf{W}^* \in \mathbb{C}^{(N-r) \times 2}$ , and that  $(\mathbf{W}^*, \mathbf{Q}^*)$  is a stationary solution to the SSRM problem (13).

The proof of Theorem 2 is identical to that of Theorem 1 and thus is omitted.

The inexact MM updating rule in (22) provides a general sufficient condition under which an algorithm can guarantee convergence to a stationary solution. The next question is how we can achieve (22) in a computationally efficient manner. This will be addressed in the next subsection.

### B. A Projected Gradient-based Inexact MM Implementation

Let us consider the following: generate an inexact solution  $\mathbf{x}^{k+1}$  to problem (21) via an iteration-limited projected gradient method (PGM). As we will see shortly, such a PGM has strong connection to the aforementioned inexact MM updating rule. The inexact PGM for problem (21) is summarized as follows:

---

#### Algorithm 1 An Inexact PGM for Problem (21)

---

- 1: Set  $l = 0$ ,  $\mathbf{x}^{k,0} = \mathbf{x}^k$  and the maximum number of PG operations  $L_k \geq 1$
  - 2: **while**  $l \leq L_k - 1$  **do**
  - 3:   Set  $\mathbf{x}^{k,l+1} = \mathbf{x}^{k,l} + \alpha^{k,l} \tilde{\nabla} \tilde{\phi}(\mathbf{x}^{k,l}; \mathbf{x}^k)$ , where  $\alpha^{k,l} > 0$  is the stepsize determined by either Armijo's rule or (limited) minimization rule [30].
  - 4:    $l = l + 1$ ;
  - 5: **end while**
  - 6:  $\mathbf{x}^{k+1} = \mathbf{x}^{k,L_k}$ .
- 

In Algorithm 1, the parameter  $L_k$  represents the maximum number of PG operations at the  $k$ th MM iteration. We see that when  $L_k = 1$  for all  $k$ , Algorithm 1 reduces to directly applying the projected gradient ascent method to the original relaxed SSRM problem (15). When  $L_k > 1$ , Algorithm 1 has an incentive to make more progress at each MM subproblem by performing multiple PG operations. Also, when every  $L_k$  approaches infinity, Algorithm 1 becomes the exact MM update, and thus the resulting MM iteration is guaranteed to converge to a stationary solution to problem (13) by Theorem 1. The following proposition reveals that the aforementioned convergence guarantee holds for any finite  $L_k$ :

**Proposition 2** Suppose that  $\{\mathbf{x}^k\}$  is a sequence generated by Algorithm 1. Then, every limit point of  $\{\mathbf{x}^k\}$  is a stationary solution to problem (15). Moreover, by using the same construction [i.e., problems (17) and (18)] as that in Theorem 1, a stationary solution to problem (13) can be extracted from every limit point of  $\{\mathbf{x}^k\}$ .

The key of the proof is to show that the iterations generated by Algorithm 1 fulfill the inequality (22). Consequently, the result follows directly from Proposition 1 and Theorem 2. The detailed proof is relegated to Appendix F.

Thus far, we have only considered convergence guarantees arising from Algorithm 1. The remaining issue is whether Algorithm 1 can be efficiently implemented. Clearly, the main computation lies in performing the PG operations, particularly, the computation of  $\tilde{\nabla} \tilde{\phi}(\mathbf{x}^{k,l}; \mathbf{x}^k)$  (cf. line 3 of Algorithm 1). From the definition of gradient mapping [cf. (20)], one needs to find an efficient way to calculate  $\mathcal{P}(\mathbf{x}^{k,l} + \nabla \tilde{\phi}(\mathbf{x}^{k,l}; \mathbf{x}^k))$ , i.e., solving the following projection problem:

$$\min_{\mathbf{W} \succeq \mathbf{0}, \mathbf{Q} \succeq \mathbf{0}} \left\| \begin{bmatrix} \mathbf{W} \\ \mathbf{Q} \end{bmatrix} - \begin{bmatrix} \mathbf{W}^{k,l} + \nabla_{\mathbf{W}} \tilde{\phi}(\mathbf{x}^{k,l}; \mathbf{x}^k) \\ \mathbf{Q}^{k,l} + \nabla_{\mathbf{Q}} \tilde{\phi}(\mathbf{x}^{k,l}; \mathbf{x}^k) \end{bmatrix} \right\|^2 \quad (23)$$

s.t.  $\text{Tr}(\mathbf{W} + \mathbf{Q}) \leq P_R, \quad \mathbf{W} \succeq \mathbf{0}, \quad \mathbf{Q} \succeq \mathbf{0}.$

Fortunately, problem (23) admits a water-filling-like solution [31, Fact 1]:

$$\mathbf{W}^* = F_1 \text{Diag}(\boldsymbol{\eta}_1^*) F_1^H, \quad \mathbf{Q}^* = F_2 \text{Diag}(\boldsymbol{\eta}_2^*) F_2^H, \quad (24)$$

where  $F_1 \text{Diag}(\tilde{\boldsymbol{\eta}}_1) F_1^H$  and  $F_2 \text{Diag}(\tilde{\boldsymbol{\eta}}_2) F_2^H$  are the eigenvalue decompositions of  $\mathbf{W}^{k,l} + \nabla_{\mathbf{W}} \tilde{\phi}(\mathbf{x}^{k,l}; \mathbf{x}^k)$  and  $\mathbf{Q}^{k,l} + \nabla_{\mathbf{Q}} \tilde{\phi}(\mathbf{x}^{k,l}; \mathbf{x}^k)$ , resp., and

$$\boldsymbol{\eta}_1^* = [\tilde{\boldsymbol{\eta}}_1 - \nu^* \mathbf{1}]^+, \quad \boldsymbol{\eta}_2^* = [\tilde{\boldsymbol{\eta}}_2 - \nu^* \mathbf{1}]^+,$$

with  $\nu^* \geq 0$  being the water-filling level. The value of  $\nu^*$  relates to the total power  $P_R$  and can be efficiently determined. Readers are referred to [31, Fact 1] for the details of solving the projection problem (23).

### C. Complexity Comparison with Exact MM

Let us analyze the computational complexities of the exact MM and the inexact MM with iteration-limited PG. While the MM subproblem (16) is convex, it is not in a standard SDP form, owing to the logarithm function  $f$ . To solve problem (16), a successive approximation method embedded with a primal-dual interior-point method (IPM) is employed, say by CVX. As is known, the arithmetic complexity for the generic primal-dual IPM to solve a standard SDP is  $\mathcal{O}(\max\{m, n\}^4 n^{1/2} \log(1/\varepsilon))$  [25], where  $m$ ,  $n$  and  $\varepsilon$  represent the number of linear constraints, the dimension of the PSD cone and the solution accuracy, resp. Therefore, for the MM subproblem (16), the per-iteration complexity is  $\mathcal{O}(L_{SA}(N-r)^{4.5} \log(1/\varepsilon))$ , where  $L_{SA}$  denotes the number of successive approximations used. On the other hand, for the PG-based inexact MM algorithm, its computation is mainly dominated by the projection operation, which involves the eigendecomposition of complexity  $\mathcal{O}((N-r)^3)$  and the water-filling level computation of complexity  $\mathcal{O}(N-r)$ . Therefore, the per-iteration complexity of PG-based inexact MM algorithm is  $\mathcal{O}(L_{PG}(N-r)^3)$ , where  $L_{PG}$  denotes the number of PG operations used for each MM subproblem. By comparing the above two complexity results, we see that the inexact MM generally has lower complexity than the exact MM, because  $L_{PG}$  is typically  $\mathcal{O}(1)$ , which is much smaller than  $L_{SA}$ .

## V. EXTENSION: SUM SECRECY RATE MAXIMIZATION UNDER AN ENERGY-HARVESTING EVE

In this section, we consider an extended scenario where the system setup and the secrecy rate model are the same as in



Sec. II, with the addition that Eve is also an energy harvesting user of the system. Thus, the relay is also required to provide certain wireless power transfer to Eve.

Under the signal model in Sec. II, the wireless power transfer from the source and the relay to Eve can be formulated as

$$\begin{aligned} p_E(\mathbf{W}_0, \mathbf{Q}_0) \\ = & \tau \left( \frac{1}{2} \mathbf{h}_{RE}^H \mathbb{E} \{ \mathbf{X}_R(n) \mathbf{X}_R(n)^H \} \mathbf{h}_{RE} + \sum_{i \in \{A, B\}} p_i |h_{iE}|^2 \right) \\ = & \tau \left( \mathbf{h}_{RE}^H (\zeta \mathbf{W}_0 \mathbf{W}_0^H + \mathbf{Q}_0) \mathbf{h}_{RE} + \sum_{i \in \{A, B\}} p_i |h_{iE}|^2 \right), \end{aligned}$$

where  $0 < \tau \leq 1$  denotes the wireless power transfer efficiency; see [15]. The subsequent SSRM problem with energy harvesting, coined SSRM-EH for short, is as follows:

$$\max_{\mathbf{Q}_0 \succeq \mathbf{0}, \mathbf{W}_0 \in \mathbb{C}^{N \times 2}} R_s(\mathbf{W}_0, \mathbf{Q}_0) \quad (25a)$$

$$\text{s.t. } p_R(\mathbf{W}_0, \mathbf{Q}_0) \leq P_R, \quad (25b)$$

$$p_E(\mathbf{W}_0, \mathbf{Q}_0) \geq \epsilon, \quad (25c)$$

$$\mathbf{H}_{RR} \mathbf{W}_0 = \mathbf{0}, \mathbf{H}_{RR} \mathbf{Q}_0 = \mathbf{0}, \quad (25d)$$

where  $\epsilon > 0$  is the minimal power transfer requirement at Eve. Similar to problem (13), the SSRM-EH problem can be equivalently written as

$$\max_{\mathbf{Q} \succeq \mathbf{0}, \mathbf{W} \in \mathbb{C}^{(N-r) \times 2}} \phi(\mathbf{W} \mathbf{W}^H, \mathbf{Q}) \quad (26a)$$

$$\text{s.t. } \text{Tr}(\mathbf{W} \mathbf{W}^H) + \text{Tr}(\mathbf{Q}) \leq P_R, \quad (26b)$$

$$\tau \mathbf{h}_{RE}^H \mathbf{V}_0 (\mathbf{W} \mathbf{W}^H + \mathbf{Q}) \mathbf{V}_0^H \mathbf{h}_{RE} \geq \tilde{\epsilon}, \quad (26c)$$

where  $\tilde{\epsilon} = \epsilon - \tau \sum_{i \in \{A, B\}} p_i |h_{iE}|^2$ . Again, the SDR-based MM approach developed in Sec. III can be employed to handle the SSRM-EH problem (26). In particular, the corresponding MM subproblem is given by

$$\begin{aligned} & (\mathbf{W}^{k+1}, \mathbf{Q}^{k+1}) \\ \in & \arg \max_{\mathbf{W} \succeq \mathbf{0}, \mathbf{Q} \succeq \mathbf{0}} \tilde{\phi}(\mathbf{W}, \mathbf{Q}; \mathbf{W}^k, \mathbf{Q}^k) \\ \text{s.t. } & \text{Tr}(\mathbf{W}) + \text{Tr}(\mathbf{Q}) \leq P_R, \\ & \tau \mathbf{h}_{RE}^H \mathbf{V}_0 (\mathbf{W} + \mathbf{Q}) \mathbf{V}_0^H \mathbf{h}_{RE} \geq \tilde{\epsilon}, \end{aligned} \quad (27)$$

where  $\tilde{\phi}$  is defined in (16a).

Let  $(\mathbf{W}, \mathbf{Q})$  be any limit point of the MM iteration in (27). Then, a stationary solution to the SSRM-EH problem (26) can be retrieved from any optimal solution to the following SDP problem:

$$\min_{\mathbf{W} \succeq \mathbf{0}, \mathbf{Q} \succeq \mathbf{0}} \text{Tr}(\mathbf{W}) + \text{Tr}(\mathbf{Q}) \quad (28a)$$

$$\text{s.t. (18b) - (18e) satisfied,} \quad (28b)$$

$$\tau \mathbf{h}_{RE}^H \mathbf{V}_0 (\mathbf{W} + \mathbf{Q}) \mathbf{V}_0^H \mathbf{h}_{RE} \geq \tilde{\epsilon}, \quad (28c)$$

Specifically, we have a similar result as Theorem 1:

**Theorem 3** *There exists an optimal solution  $(\mathbf{W}^*, \mathbf{Q}^*)$  to problem (28) such that  $\text{rank}(\mathbf{W}^*) \leq 2$ ; i.e.,  $\mathbf{W}^*$  can be decomposed as  $\mathbf{W}^* \mathbf{W}^{*H}$  for some  $\mathbf{W}^* \in \mathbb{C}^{(N-r) \times 2}$ . Also,  $(\mathbf{W}^*, \mathbf{Q}^*)$  is a stationary solution or KKT solution to problem (26).*

*Proof.* See Appendix G. ■

In addition, the inexact MM update in Algorithm 1 can also be applied to the SSRM-EH problem (26) with the gradient projection step modified as

$$\min_{\mathbf{W} \succeq \mathbf{0}, \mathbf{Q} \succeq \mathbf{0}} \theta(\mathbf{W}, \mathbf{Q}) \triangleq \left\| \begin{bmatrix} \mathbf{W} \\ \mathbf{Q} \end{bmatrix} - \begin{bmatrix} \mathbf{W}^{k,l} + \nabla_{\mathbf{W}} \tilde{\phi}(\mathbf{x}^{k,l}; \mathbf{x}^k) \\ \mathbf{Q}^{k,l} + \nabla_{\mathbf{Q}} \tilde{\phi}(\mathbf{x}^{k,l}; \mathbf{x}^k) \end{bmatrix} \right\|^2 \quad (29a)$$

$$\text{s.t. } \text{Tr}(\mathbf{W} + \mathbf{Q}) \leq P_R, \quad (29b)$$

$$\tau \mathbf{h}_{RE}^H \mathbf{V}_0 (\mathbf{W} + \mathbf{Q}) \mathbf{V}_0^H \mathbf{h}_{RE} \geq \tilde{\epsilon}. \quad (29c)$$

By invoking the solution in (24), problem (29) can be efficiently solved using the dual ascent method [30]. In particular, let  $\lambda \geq 0$  be the dual variable associated with (29c). The dual of problem (29) is given by

$$\max_{\lambda \geq 0} d(\lambda),$$

where

$$d(\lambda) \triangleq$$

$$\begin{aligned} & \min_{\mathbf{W}, \mathbf{Q}} \theta(\mathbf{W}, \mathbf{Q}) - \lambda (\tau \text{Tr}((\mathbf{W} + \mathbf{Q}) \mathbf{V}_0^H \mathbf{h}_{RE} \mathbf{h}_{RE}^H \mathbf{V}_0) - \tilde{\epsilon}) \\ & \text{s.t. } \text{Tr}(\mathbf{W} + \mathbf{Q}) \leq P_R, \mathbf{W} \succeq \mathbf{0}, \mathbf{Q} \succeq \mathbf{0}. \end{aligned} \quad (30)$$

Given  $\lambda$ , problem (30) can be written into a form like problem (23), and thus has a solution like (24). Moreover, the optimal dual variable can be computed by using bisection to search for a  $\lambda^* \geq 0$  such that the complementarity condition for the constraint (29c) is satisfied.

## VI. NUMERICAL RESULTS

In this section, we use Monte Carlo simulations to evaluate the performances of the proposed SSRM algorithms.

### A. The Case of No Energy Harvesting with Eve

We consider the scenario in Sec. II and the SSRM approach in Secs. III–IV. The results to be presented in this subsection are based on the following simulation settings, unless otherwise specified: The number of transmit antennas and receive antennas at the relay are  $N = 6$  and  $M = 3$ , resp.; all the channels are randomly generated following i.i.d. complex Gaussian distribution with zero mean and unit variance; the receive noise at each node has the same unit variance, i.e.,  $\sigma_A^2 = \sigma_B^2 = \sigma_E^2 = \sigma_R^2 = 1$ ; both Alice and Bob have the same full-duplex SI residual factor  $\kappa_A = \kappa_B = \kappa$  and the same transmit power  $p_A = p_B$ .

1) *Exact and Inexact MM Comparisons:* Fig. 2 shows the convergence behaviors of the exact MM and the inexact MM (In-MM) algorithms under one problem instance. Specifically, the exact MM solves the problem (16) exactly with CVX [26] (thus named “MM-CVX”). The inexact MM approximately solves the problem (16) by Algorithm 1, with  $L_k = L$  for all  $k$  and with the stepsize  $\alpha^{k,l}$  determined by Armijo’s rule. Both the exact and inexact MMs are initialized by  $\mathbf{W}^0 = \mathbf{Q}^0 = \frac{P_R}{2(N-r)} \mathbf{I}$ . The stopping criterion for MM-CVX is  $|\tilde{\phi}(\mathbf{x}^{\bar{k}}; \mathbf{x}^{\bar{k}-1}) - \tilde{\phi}(\mathbf{x}^{\bar{k}-1}; \mathbf{x}^{\bar{k}-2})| / |\tilde{\phi}(\mathbf{x}^{\bar{k}-1}; \mathbf{x}^{\bar{k}-2})| < 10^{-3}$  for some  $\bar{k}$ , and the stopping criterion for In-MM is that the



In-MM iterate attains the same objective value  $\tilde{\phi}(\mathbf{x}^k; \mathbf{x}^{k-1})$  as the MM-CVX after convergence. In Fig. 2, we also considered In-MMs with different number of PG operations  $L$ , including fixed  $L = 1, 3, 5$  and variable  $L$  which is randomly and uniformly chosen from 1 to 5 at each MM iteration. As seen, the sum secrecy rates of both the exact and inexact MM increase with the number of iterations, and converge to about 2 nats/s/Hz. The exact MM converges in 4 iterations, which is very fast. Also, the inexact MM need more iterations to converge, varying from 7 iterations (w.r.t.  $L = 5$ ) to 90 iterations (w.r.t.  $L = 1$ ), which is expected.

Since the per-iteration complexities of the exact MM and inexact MM are different, a fairer comparison is to measure their running times. Fig. 3 plots the running times of In-MMs (normalized by the time of MM-CVX at convergence) when In-MMs achieve  $\alpha\tilde{\phi}(\mathbf{x}^k; \mathbf{x}^{k-1})$  for  $\alpha = 0.1 \sim 1$  under the same setting as Fig. 2. It is clear that In-MMs run much faster than MM-CVX. Moreover, In-MM with variable  $L$  is seen to be more efficient than that with fixed  $L$ . The reason for this is as follows: The inexact MM algorithm involves two loops, namely, the outer MM iterations and the inner iteration-limited PG operations. Therefore, the total computational complexity equals the complexity of the inner PG operations times the total number of outer MM iterations. From Fig. 2, we see that the more PG operations performed for the inner loop, the less MM iterations for the outer, and vice versa. Therefore, there is a trade off between the solution inexactness and the number of outer MM iterations. From Fig. 3, it seems that choosing  $L$  uniformly and randomly may get a better balance of these two.

2) *Secrecy Rates Versus the Source Power*: We study the relationship between the source power and the sum secrecy rate performance under different SI residual level  $\kappa$ . For comparison, we also considered the half-duplex two-way relay designs, where Alice, Bob and the relay are all half duplex. In such a case, there is no SI at the each node, but the rate suffers from a reduction by a half. One can check that the SDR-based MM approach developed in this paper is still applicable by setting  $\kappa_A = \kappa_B = 0$ , removing the zero-forcing constraint (12c), lifting the variable dimension of  $\mathbf{W}$  and  $\mathbf{Q}$  from  $(N-r) \times (N-r)$  to  $N \times N$  and modifying Eve's sum rate accordingly.<sup>3</sup> Fig. 4 shows the result, where "FD" and "HD" correspond to the full-duplex and half duplex-based designs, resp. From these figures, we have the following observations. Firstly, we observe that the sum secrecy rate of FD is generally better than that of HD. The reason for this is two-fold: 1) The HD protocol suffers from half rate reduction; 2) The existence of the direct links makes the HD more vulnerable

<sup>3</sup>Under the half-duplex case, the received signal models at Alice, Bob and Eve are the same as before, except for the noise covariance in (7), which is changed as

$$\Psi = \begin{bmatrix} \tilde{\sigma}_R^2 \|\mathbf{h}_{RE}^H \mathbf{W}_0\|^2 + \mathbf{h}_{RE}^H \mathbf{Q}_0 \mathbf{h}_{RE} + \sigma_E^2 & \\ & \sigma_E^2 \end{bmatrix}.$$

Hence, the Eve's sum rate is calculated accordingly as

$$\begin{aligned} R_E(\mathbf{W}_0, \mathbf{Q}_0) &= \log \left( (\sigma_E^2 \tilde{\sigma}_R^2 + \theta_1 \tilde{\sigma}_R^2 + \sigma_E^2 \sum_{i \in \{A, B\}} \tilde{p}_i + \theta_2) \|\mathbf{h}_{RE}^H \mathbf{W}_0\|^2 + (\theta_1 + \sigma_E^2) \mathbf{h}_{RE}^H \mathbf{Q}_0 \mathbf{h}_{RE} + \sigma_E^4 + \sigma_E^2 \theta_1 \right) \\ &- \log \left( \sigma_E^2 \tilde{\sigma}_R^2 \|\mathbf{h}_{RE}^H \mathbf{W}_0\|^2 + \sigma_E^2 \mathbf{h}_{RE}^H \mathbf{Q}_0 \mathbf{h}_{RE} + \sigma_E^4 \right). \end{aligned}$$

to interception than the FD, as the direct links of the former are free of interference, whereas for the FD case, they are interfered by the relay-to-Eve link, which somehow can better protect the sources' transmissions. Second, the sum secrecy rates of FD and HD both first increase with the source power, and then decrease when the source power is higher than a certain level. For the FD case, this is because the residual SI increases with the source power and can compensate any SINR gains obtained from transmit optimization; while for the HD case, this behavior is owing to the improved interception quality from the direct links.

3) *Secrecy Rates Versus the Number of Relay's Transmit Antenna*: In this example, we study the relationship between the sum secrecy rate and the number of transmit antennas  $N$  at the relay. The result is shown in Fig. 5. As seen, for  $N \leq 3$  FD cannot provide positive secrecy rate, owing to the ZF constraints (recall the number of receive antennas at relay is 3). However, when  $N$  increases, the effect of ZF constraint becomes less, and the benefit of exploiting FD (or the temporal degrees of freedom (TDoF) with STR) outweighs the loss of the spatial DoF (SDoF).

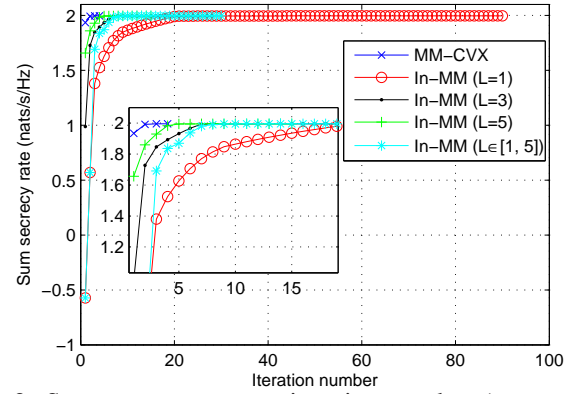


Fig. 2: Sum secrecy rate vs. iteration number ( $p_A = p_B = P_R = 10\text{dB}$ ,  $\kappa = 0.1$ ).

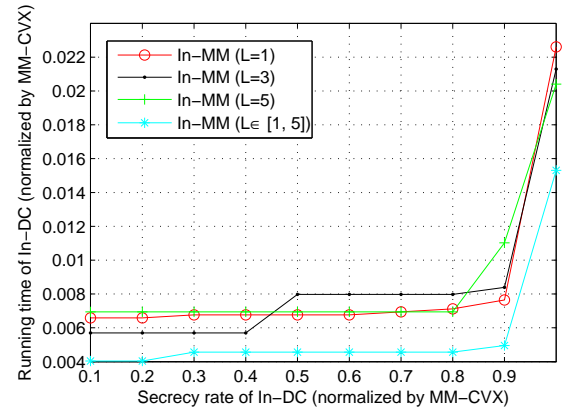


Fig. 3: Running time comparison ( $p_A = p_B = P_R = 10\text{dB}$ ,  $\kappa = 0.1$ ).

## B. The Energy-Harvesting Eve Case

We consider the energy-harvesting Eve extension in Sec. V. The simulation settings are basically the same as before, i.e.,

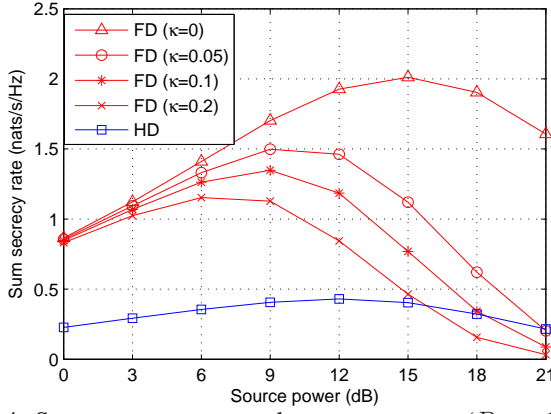


Fig. 4: Sum secrecy rate vs. the source power ( $P_R = 10\text{dB}$ ).

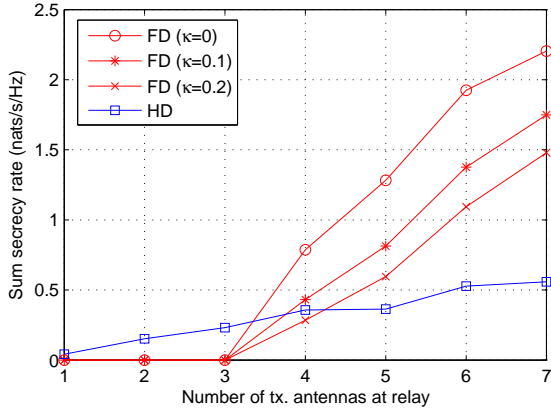


Fig. 5: Sum secrecy rate vs. the number of tx. antennas at the relay ( $p_A = p_B = p_R = 10\text{dB}$ ).

$N = 6$ ,  $M = 3$ ,  $p_A = p_B$ ,  $\kappa_A = \kappa_B = \kappa$ , but with the following modifications, which are adopted to better capture the power transfer scenario: The noise variance at each node is the same and equals  $-50\text{dBm}$ . All the channels follow complex Gaussian distribution with mean zero. The variance of Eve's channel is set to  $-10\text{dB}$ , and that of all the others' channels to  $-20\text{dB}$ ; i.e., Eve is on average closer to the relay in order to better receive energy. The power transfer efficiency is  $\tau = 10\%$ .

#### 1) Secrecy Rates Versus the Power Transfer Threshold:

Let us first study the achievable rate-power region of the proposed design for different residual SI factor  $\kappa$ . The result is shown in Fig. 6. For comparison, we also plotted the result of the HD design. From the figure, we see that the rate-power region shrinks when the residual SI level increases. Moreover, compared with the HD design, the FD design is able to attain larger secrecy rate when SI is well suppressed, but its maximal power transfer ability is inferior to the HD design. This is because the FD design sacrifices the SDoF in order to better exploit the TDoF. However, for the power transfer constraint in (26c), such SDoF loss would have impact on the maximal power transfer ability, as can be seen from

$$\tau \mathbf{h}_{RE}^H \mathbf{V}_0 (\mathbf{W} + \mathbf{Q}) \mathbf{V}_0^H \mathbf{h}_{RE} \leq \tau P_R \|\mathbf{V}_0^H \mathbf{h}_{RE}\|^2 < \tau P_R \|\mathbf{h}_{RE}\|^2$$

where the first inequality is due to the total power constraint at the relay, and the last inequality follows from the fact that  $\mathbf{V}_0$  is a semi-unitary matrix.

2) *The Importance of Artificial Noise:* In this example, we examine when AN is crucial for the design. To this end, we consider the same setting as Fig. 6 and measure the ratio of AN's power to the total transmit power at the relay under different power transfer requirement  $\epsilon$ . The result is shown in Fig. 7. From the figure, we see that for both FD and HD, the percentages of AN's power first increase and then decrease, when Eve's power transfer requirement increases. This phenomenon reveals an interesting result — For extremely loose or stringent power requirements, AN is not crucial. However, for moderate operational regions, AN is important. This may be explained as follows: For very small  $\epsilon$ , a small portion of AN already fulfills Eve's power transfer requirement, and there is no need to further waste power on AN. With the increase of power transfer requirement, more power needs to be allocated to Eve, and it is reasonable to use AN to fulfill this need since it also jams Eve's reception. However, when the power transfer requirement becomes extremely stringent, the relay has to align the transmit signal around Eve (to make problem (25) feasible), which in turn may result in low reception power at the legitimate nodes. In other words, to Alice and Bob, the relay virtually works in a low transmission power regime. For such a power limited regime, more power should be allocated to information symbols to achieve higher secrecy rate.

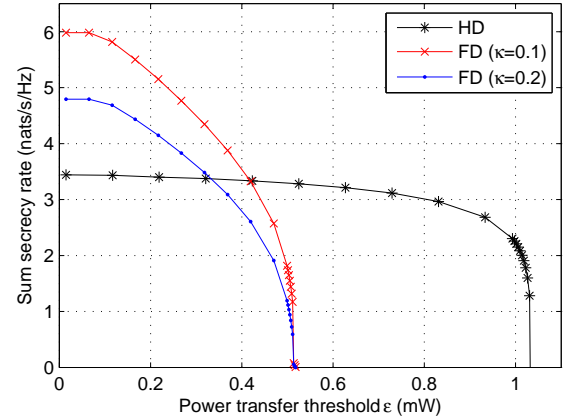


Fig. 6: Power transfer level vs. sum secrecy rate ( $p_A = p_B = P_R = 10\text{dBm}$ ).

## VII. CONCLUSION

In this paper we have considered the sum secrecy rate maximization (SSRM)-based transmit optimization for full-duplex two-way relaying communications. A minorization-maximization (MM) approach was proposed for the SSRM problem. We prove that convergence to a stationary solution to the SSRM problem is guaranteed with either exact or inexact MM updates, as long as certain solution inexactness condition is satisfied throughout the iterations. Extension to the case of energy-harvesting Eve was also considered.

## VIII. ACKNOWLEDGEMENT

The authors would like to thank the anonymous reviewers for their valuable comments which are helpful in improving this paper.

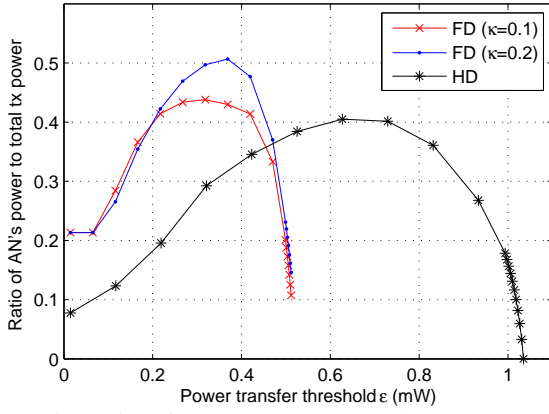


Fig. 7: The ratio of AN's power to total tx. power at relay for different power transfer threshold  $\epsilon$  ( $p_A = p_B = p_R = 10\text{dBm}$ ).

## APPENDIX

### A. Derivation of Eve's Reception Model

Let us focus on the reception of  $s_A(2n-1)$  and  $s_B(2n-1)$  from  $\mathbf{y}_E(n)$  and  $\mathbf{y}_E(n-1)$ . For  $\mathbf{y}_E(n)$ , we apply the standard Alamouti reception to retrieve a sample, denoted herein by  $\tilde{y}_{E,1}(n)$ , that corresponds to the reception of  $s_A(2n-1)$  and  $s_B(2n-1)$ . Following the model of  $\mathbf{y}_E(n)$  in (6), one can show the expression of  $\tilde{y}_{E,1}(n)$  in (31), where  $[\mathbf{h}_{RE}^H \mathbf{W}_0]_\ell$  denotes the  $\ell$ th element of  $\mathbf{h}_{RE}^H \mathbf{W}_0$ . For  $\mathbf{y}_E(n-1)$ , observe from (6) that  $s_A(2n-1)$  and  $s_B(2n-1)$  appears only in the first element of  $\mathbf{y}_E(n-1)$ . By letting  $\tilde{y}_{E,2}(n) = [\mathbf{y}_E(n-1)]_1$ , and following (6), the expression of  $\tilde{y}_{E,2}(n)$  can be obtained and it is shown in (32). By stacking the two samples as  $\tilde{\mathbf{y}}_E(n) = [\tilde{y}_{E,1}(n) \ \tilde{y}_{E,2}(n)]^T$ , it can be shown from (31)–(32) that

$$\tilde{\mathbf{y}}(n) = \mathbf{H}_E \begin{bmatrix} s_A(2n-1) \\ s_B(2n-1) \end{bmatrix} + \tilde{\mathbf{n}}_E(n),$$

where  $\mathbf{H}_E$  and  $\tilde{\mathbf{n}}_E(n)$  are defined in (7).

Also, the reception of  $s_A(2n)$  and  $s_B(2n)$  from  $\mathbf{y}_E(n)$  and  $\mathbf{y}_E(n-1)$  follows the same derivations as above. Thus, we conclude that (7) provides an equivalent MIMO model for Eve's reception.

### B. Derivation of Eve's Sum Achievable Rate

The sum achievable rate (10) at Eve can be further derived as (33), where  $\theta_1$  and  $\theta_2$  are defined in (11). To express  $R_E(\mathbf{W}_0, \mathbf{Q}_0)$  as (11), notice from the definitions of  $\Psi_{11}$  and  $\Psi_{22}$  in (8) that  $\Psi_{11} = \Psi_{22} - \|\mathbf{h}_{RE}^H \mathbf{W}_0\|^2(\tilde{p}_A + \tilde{p}_B) + \sum_{i \in \{A,B\}} p_i |h_{iE}|^2$ . Hence,

$$\begin{aligned} & \Psi_{11} \Psi_{22} \\ &= \Psi_{22}^2 - \|\mathbf{h}_{RE}^H \mathbf{W}_0\|^2(\tilde{p}_A + \tilde{p}_B)\Psi_{22} + \sum_{i \in \{A,B\}} p_i |h_{iE}|^2 \Psi_{22} \\ &= \Psi_{22}^2 - \|\mathbf{h}_{RE}^H \mathbf{W}_0\|^2(\sum_{i \in \{A,B\}} p_i |\tilde{f}_{iR}|^2) \Psi_{22} + \theta_1 \Psi_{22}, \end{aligned} \quad (34)$$

where the second equality is due to  $\tilde{p}_i = p_i |\tilde{f}_{iR}|^2$  (cf. the definitions of  $\tilde{p}_i$  and  $\tilde{f}_{iR}$  for  $i \in \{A,B\}$ ). Now, by substituting

(34) into (33), we obtain

$$\begin{aligned} & R_E(\mathbf{W}_0, \mathbf{Q}_0) \\ &= \log \left( \frac{\Psi_{22}^2 + \theta_1(\Psi_{22} + \Psi_{11}) + \theta_2 \|\mathbf{h}_{RE}^H \mathbf{W}_0\|^2}{\Psi_{11} \Psi_{22}} \right). \end{aligned}$$

### C. Proof of Lemma 1

Since  $\tilde{g}_1(\mathbf{W}, \mathbf{Q}; \mathbf{W}^k, \mathbf{Q}^k)$  and  $\tilde{g}_2(\mathbf{W}, \mathbf{Q}; \mathbf{W}^k, \mathbf{Q}^k)$  are convex upper bounds of  $g_1(\mathbf{W}, \mathbf{Q})$  and  $g_2(\mathbf{W}, \mathbf{Q})$ , resp., which is tight at  $(\mathbf{W}^k, \mathbf{Q}^k)$ , it follows from the basic MM property that

$$\begin{aligned} \phi(\mathbf{W}^k, \mathbf{Q}^k) &= \tilde{\phi}(\mathbf{W}^k, \mathbf{Q}^k; \mathbf{W}^k, \mathbf{Q}^k) \\ &\leq \tilde{\phi}(\mathbf{W}^{k+1}, \mathbf{Q}^{k+1}; \mathbf{W}^k, \mathbf{Q}^k) \\ &\leq \phi(\mathbf{W}^{k+1}, \mathbf{Q}^{k+1}) \\ &\vdots \\ &\leq \phi(\bar{\mathbf{W}}, \bar{\mathbf{Q}}), \end{aligned}$$

i.e.,  $\{\tilde{\phi}(\mathbf{W}^{k+1}, \mathbf{Q}^{k+1}; \mathbf{W}^k, \mathbf{Q}^k)\}_k$  converges monotonically to the upper bound  $\phi(\bar{\mathbf{W}}, \bar{\mathbf{Q}})$ . By noting the continuity of the function  $\tilde{\phi}$ , and taking a convergent subsequence of  $\{(\mathbf{W}^k, \mathbf{Q}^k)\}_k$  with a limit point  $(\bar{\mathbf{W}}, \bar{\mathbf{Q}})$ , we have

$$\tilde{\phi}(\mathbf{W}, \mathbf{Q}; \bar{\mathbf{W}}, \bar{\mathbf{Q}}) \leq \phi(\bar{\mathbf{W}}, \bar{\mathbf{Q}})$$

for all feasible  $(\mathbf{W}, \mathbf{Q})$ . In addition, from the definition of  $\tilde{\phi}$ , we have  $\tilde{\phi}(\bar{\mathbf{W}}, \bar{\mathbf{Q}}; \bar{\mathbf{W}}, \bar{\mathbf{Q}}) = \phi(\bar{\mathbf{W}}, \bar{\mathbf{Q}})$ . Thus,  $(\bar{\mathbf{W}}, \bar{\mathbf{Q}})$  is an optimal solution to problem (17).

On the other hand from the construction of problem (18), one can easily show that every optimal  $(\mathbf{W}^*, \mathbf{Q}^*)$  of (18) must be feasible for problem (17) with  $\tilde{\phi}(\mathbf{W}^*, \mathbf{Q}^*; \bar{\mathbf{W}}, \bar{\mathbf{Q}}) = \phi(\bar{\mathbf{W}}, \bar{\mathbf{Q}}; \bar{\mathbf{W}}, \bar{\mathbf{Q}})$ . Hence, every optimal  $(\mathbf{W}^*, \mathbf{Q}^*)$  of (18) is optimal for (17).

### D. Proof of Theorem 1

Notice that problem (18) is an SDP with 7 constraints. By the SDP rank-reduction result in [28, Lemma 3.1], there exists an optimal solution  $(\mathbf{W}^*, \mathbf{Q}^*)$  to problem (18) such that

$$\text{rank}(\mathbf{W}^*)^2 + \text{rank}(\mathbf{Q}^*)^2 \leq 7,$$

which implies that

$$\text{rank}(\mathbf{W}^*) \leq \sqrt{7} < 3$$

Hence,  $\text{rank}(\mathbf{W}^*)$  equals 1 or 2, and by Lemma 1 such an optimal  $(\mathbf{W}^*, \mathbf{Q}^*)$  is also optimal for problem (17). Next, we establish the second part of the Theorem.

Since  $(\mathbf{W}^*, \mathbf{Q}^*)$  is an optimal solution to problem (17), it satisfies the KKT conditions of problem (17). To describe it, let us denote  $\gamma \geq 0$ ,  $\mathbf{Y} \succeq \mathbf{0}$  and  $\mathbf{Z} \succeq \mathbf{0}$  as the dual variables associated with the power constraint,  $\mathbf{W}^* \succeq \mathbf{0}$  and  $\mathbf{Q}^* \succeq \mathbf{0}$  of problem (17). Then, the KKT conditions of problem (17) are shown in (35), where for notational simplicity we have dropped all the arguments and used  $(\cdot)^*$  [resp.  $(\cdot)$ ] to represent the function value or gradient evaluation at the point  $(\mathbf{W}^*, \mathbf{Q}^*)$  [resp.  $(\mathbf{W}, \mathbf{Q})$ ].

Since  $\beta_i^* = \beta_i$  and  $\psi_i^* = \psi_i$  for all  $i$  [cf. problem (18)], and  $\nabla_{\mathbf{W}} \beta_i$ ,  $\nabla_{\mathbf{Q}} \beta_i$  are constant matrices, irrespective of  $(\mathbf{W}, \mathbf{Q})$ ,



$$\begin{aligned}
\tilde{y}_{E,1}(n) = & \| \mathbf{h}_{RE}^H \mathbf{W}_0 \| \left\{ \sum_{i \in \{A,B\}} (\mathbf{f}_A + \mathbf{f}_B)^H \mathbf{h}_{iR} s_i(2n-1) + (\mathbf{f}_A + \mathbf{f}_B)^H \mathbf{n}_R(2n-1) \right\} + \\
& \frac{1}{\| \mathbf{h}_{RE}^H \mathbf{W}_0 \|} \left\{ [\mathbf{h}_{RE}^H \mathbf{W}_0]_1 \left( \mathbf{h}_{RE}^H \mathbf{z}(2n-1) + n_E(2n+1) + \sum_{i \in \{A,B\}} \mathbf{h}_{iE} s_i(2n+1) \right) - \right. \\
& \left. [\mathbf{h}_{RE}^H \mathbf{W}_0]_2^* \left( \mathbf{h}_{RE}^T \mathbf{z}^*(2n) + n_E^*(2n+2) + \sum_{i \in \{A,B\}} \mathbf{h}_{iE}^* s_i^*(2n+2) \right) \right\}
\end{aligned} \tag{31}$$


---

$$\begin{aligned}
\tilde{y}_{E,2}(n) = & \sum_{i \in \{A,B\}} h_{iE} s_i(2n-1) + \mathbf{h}_{RE}^H \mathbf{z}(2n-3) + n_E(2n-1) + \\
& [\mathbf{h}_{RE}^H \mathbf{W}_0]_1 \left\{ \sum_{i \in \{A,B\}} (\mathbf{f}_A + \mathbf{f}_B)^H \mathbf{h}_{iR} s_i(2n-3) + (\mathbf{f}_A + \mathbf{f}_B)^H \mathbf{n}_R(2n-3) \right\} + \\
& [\mathbf{h}_{RE}^H \mathbf{W}_0]_2^* \left\{ \sum_{i \in \{A,B\}} (\mathbf{f}_A + \mathbf{f}_B)^H \mathbf{h}_{iR} s_i(2n-2) + (\mathbf{f}_A + \mathbf{f}_B)^H \mathbf{n}_R(2n-2) \right\}
\end{aligned} \tag{32}$$


---

$$\begin{aligned}
& R_E(\mathbf{W}_0, \mathbf{Q}_0) \\
& = \log |\mathbf{I} + \mathbf{H}_E \mathbf{P} \mathbf{H}_E^H \Psi^{-1}| \\
& = \log \left| 1 + \frac{\| \mathbf{h}_{RE}^H \mathbf{W}_0 \|^2 (\sum_{i \in \{A,B\}} p_i |\tilde{f}_{iR}|^2)}{\Psi_{11}} \frac{\| \mathbf{h}_{RE}^H \mathbf{W}_0 \| \sum_{i \in \{A,B\}} \tilde{f}_{iR} h_{iE}^*}{\Psi_{22}} \right| \\
& = \log \left( \frac{\Psi_{11} \Psi_{22} + \| \mathbf{h}_{RE}^H \mathbf{W}_0 \|^2 (\sum_{i \in \{A,B\}} p_i |\tilde{f}_{iR}|^2) \Psi_{22} + \theta_1 \Psi_{11} + \theta_2 \| \mathbf{h}_{RE}^H \mathbf{W}_0 \|^2}{\Psi_{11} \Psi_{22}} \right)
\end{aligned} \tag{33}$$


---

$$\sum_{i=1}^2 \frac{\nabla \mathbf{w} \alpha_i^*}{c_i + \alpha_i^*} + \sum_{i=1}^2 \frac{\nabla \mathbf{w} \psi_i^*}{\psi_i^*} - \sum_{i=1}^2 \frac{\nabla \mathbf{w} \bar{\beta}_i}{c_i + \bar{\beta}_i} - \frac{2\psi_2^* \nabla \mathbf{w} \psi_2^* + \theta_1 (\nabla \mathbf{w} \psi_1^* + \nabla \mathbf{w} \psi_2^*) + \theta_2 \zeta^{-1} \mathbf{V}_0^H \mathbf{h}_{RE} \mathbf{h}_{RE}^H \mathbf{V}_0}{(\psi_2^*)^2 + \theta_1 (\psi_1^* + \psi_2^*) + \theta_2 \zeta^{-1} \mathbf{h}_{RE}^H \mathbf{V}_0 \mathbf{W} \mathbf{V}_0^H \mathbf{h}_{RE}} - \gamma \mathbf{I} + \mathbf{Y} = \mathbf{0}, \tag{35a}$$

$$\sum_{i=1}^2 \frac{\nabla \mathbf{Q} \alpha_i^*}{c_i + \alpha_i^*} + \sum_{i=1}^2 \frac{\nabla \mathbf{Q} \psi_i^*}{\psi_i^*} - \sum_{i=1}^2 \frac{\nabla \mathbf{Q} \bar{\beta}_i}{c_i + \bar{\beta}_i} - \frac{2\psi_2^* \nabla \mathbf{Q} \psi_2^* + \theta_1 (\nabla \mathbf{Q} \psi_1^* + \nabla \mathbf{Q} \psi_2^*)}{(\bar{\psi}_2)^2 + \theta_1 (\bar{\psi}_1 + \bar{\psi}_2) + \theta_2 \zeta^{-1} \mathbf{h}_{RE}^H \mathbf{V}_0 \bar{\mathbf{W}} \mathbf{V}_0^H \mathbf{h}_{RE}} - \gamma \mathbf{I} + \mathbf{Z} = \mathbf{0}, \tag{35b}$$

$$\text{Tr}(\mathbf{W}^* + \mathbf{Q}^*) \leq P_R, \quad \mathbf{Q}^* \succeq \mathbf{0}, \quad \gamma \geq 0, \tag{35c}$$

$$\mathbf{Q}^* \mathbf{Z} = \mathbf{0}, \quad \mathbf{Z} \succeq \mathbf{0}, \tag{35d}$$

$$\mathbf{Y} \mathbf{W}^* = \mathbf{0}, \quad \mathbf{Y} \succeq \mathbf{0}, \quad \mathbf{W}^* \succeq \mathbf{0}. \tag{35e}$$


---

$$\sum_{i=1}^2 \frac{\nabla \mathbf{w} \alpha_i^*}{c_i + \alpha_i^*} + \sum_{i=1}^2 \frac{\nabla \mathbf{w} \psi_i^*}{\psi_i^*} - \sum_{i=1}^2 \frac{\nabla \mathbf{w} \beta_i^*}{c_i + \beta_i^*} - \frac{2\psi_2^* \nabla \mathbf{w} \psi_2^* + \theta_1 (\nabla \mathbf{w} \psi_1^* + \nabla \mathbf{w} \psi_2^*) + \theta_2 \zeta^{-1} \mathbf{V}_0^H \mathbf{h}_{RE} \mathbf{h}_{RE}^H \mathbf{V}_0}{(\psi_2^*)^2 + \theta_1 (\psi_1^* + \psi_2^*) + \theta_2 \zeta^{-1} \mathbf{h}_{RE}^H \mathbf{V}_0 \mathbf{W}^* \mathbf{V}_0^H \mathbf{h}_{RE}} - \gamma \mathbf{I} + \mathbf{Y} = \mathbf{0}, \tag{36a}$$

$$\sum_{i=1}^2 \frac{\nabla \mathbf{Q} \alpha_i^*}{c_i + \alpha_i^*} + \sum_{i=1}^2 \frac{\nabla \mathbf{Q} \psi_i^*}{\psi_i^*} - \sum_{i=1}^2 \frac{\nabla \mathbf{Q} \beta_i^*}{c_i + \beta_i^*} - \frac{2\psi_2^* \nabla \mathbf{Q} \psi_2^* + \theta_1 (\nabla \mathbf{Q} \psi_1^* + \nabla \mathbf{Q} \psi_2^*)}{(\psi_2^*)^2 + \theta_1 (\psi_1^* + \psi_2^*) + \theta_2 \zeta^{-1} \mathbf{h}_{RE}^H \mathbf{V}_0 \mathbf{W}^* \mathbf{V}_0^H \mathbf{h}_{RE}} - \gamma \mathbf{I} + \mathbf{Z} = \mathbf{0}. \tag{36b}$$


---

Eq. (35a) and (35b) can be reexpressed as (36a) and (36b), from (35e) that

resp. Moreover, from the previous proof, we have shown that  $\text{rank}(\mathbf{W}^*) \leq 2$ . Thus,  $\mathbf{W}^*$  can be decomposed as  $\mathbf{W}^* = \mathbf{W}^* \mathbf{W}^{*H}$  for some  $\mathbf{W}^* \in \mathbb{C}^{(N-r) \times 2}$ . It thus follows

$$\mathbf{Y} \mathbf{W}^* \mathbf{W}^{*H} = \mathbf{0} \iff \mathbf{Y} \mathbf{W}^* = \mathbf{0}. \tag{37}$$

By postmultiplying the both sides of (36a) with  $2\mathbf{W}^*$ , and

$$\begin{aligned}
& \sum_{i=1}^2 \frac{2\nabla_{\mathbf{W}} \alpha_i^* \mathbf{W}^*}{c_i + \alpha_i^*} + \sum_{i=1}^2 \frac{2\nabla_{\mathbf{W}} \psi_i^* \mathbf{W}^*}{\psi_i^*} - \sum_{i=1}^2 \frac{2\nabla_{\mathbf{W}} \beta_i^* \mathbf{W}^*}{c_i + \beta_i^*} \\
& - \frac{4\psi_2^* \nabla_{\mathbf{W}} \psi_2^* \mathbf{W}^* + 2\theta_1 (\nabla_{\mathbf{W}} \psi_1^* + \nabla_{\mathbf{W}} \psi_2^*) \mathbf{W}^* + 2\theta_2 \zeta^{-1} \mathbf{V}_0^H \mathbf{h}_{RE} \mathbf{h}_{RE}^H \mathbf{V}_0 \mathbf{W}^*}{(\psi_2^*)^2 + \theta_1 (\psi_1^* + \psi_2^*) + \theta_2 \zeta^{-1} \mathbf{h}_{RE}^H \mathbf{V}_0 \mathbf{W}^* \mathbf{W}^{*H} \mathbf{V}_0^H \mathbf{h}_{RE}} = 2\gamma \mathbf{W}^*
\end{aligned} \tag{38}$$

using (37), we arrive at (38). Moreover, one can verify that the following equations hold:

$$\begin{aligned}
2\nabla_{\mathbf{W}} \alpha_i(\mathbf{W}^*, \mathbf{Q}^*) \mathbf{W}^* &= \nabla_{\mathbf{W}} \alpha_i(\mathbf{W}^* \mathbf{W}^{*H}, \mathbf{Q}^*) \quad i = 1, 2, \\
2\nabla_{\mathbf{W}} \beta_i(\mathbf{W}^*, \mathbf{Q}^*) \mathbf{W}^* &= \nabla_{\mathbf{W}} \beta_i(\mathbf{W}^* \mathbf{W}^{*H}, \mathbf{Q}^*) \quad i = 1, 2, \\
2\nabla_{\mathbf{W}} \psi_i(\mathbf{W}^*, \mathbf{Q}^*) \mathbf{W}^* &= \nabla_{\mathbf{W}} \psi_i(\mathbf{W}^* \mathbf{W}^{*H}, \mathbf{Q}^*), \quad i = 1, 2.
\end{aligned} \tag{39}$$

By substituting (39) into (38), and by replacing  $\mathbf{W}^*$  with  $\mathbf{W}^* \mathbf{W}^{*H}$  in (35c) and (36b), we see that (35c), (35d), (36b) and (38) exactly constitute the KKT conditions of problem (13). Therefore,  $(\mathbf{W}^*, \mathbf{Q}^*)$ , together with the dual variables  $\gamma, \mathbf{Z}$ , forms a KKT point of problem (13).

#### E. Proof of Proposition 1

Recall  $\phi(\mathbf{x}^{k+1}) \geq \tilde{\phi}(\mathbf{x}^{k+1}; \mathbf{x}^k)$  and  $\phi(\mathbf{x}^k) = \tilde{\phi}(\mathbf{x}^k; \mathbf{x}^k)$ . We have

$$\begin{aligned}
\phi(\mathbf{x}^{k+1}) - \phi(\mathbf{x}^k) &\geq \tilde{\phi}(\mathbf{x}^{k+1}; \mathbf{x}^k) - \tilde{\phi}(\mathbf{x}^k; \mathbf{x}^k) \\
&\geq \zeta^k \|\tilde{\nabla} \tilde{\phi}(\mathbf{x}^k; \mathbf{x}^k)\|^2 \\
&\geq 0,
\end{aligned}$$

i.e.,  $\{\phi(\mathbf{x}^k)\}$  is nondecreasing. Taking summation on both sides of the above inequality over  $k$  from 0 to  $K-1$  yields

$$\phi(\mathbf{x}^K) - \phi(\mathbf{x}^0) \geq \sum_{k=0}^{K-1} \zeta^k \|\tilde{\nabla} \tilde{\phi}(\mathbf{x}^k; \mathbf{x}^k)\|^2.$$

Since  $\mathcal{D}$  is compact and  $\phi$  is continuous,  $\phi(\mathbf{x}^K) - \phi(\mathbf{x}^0)$  is bounded from above. Moreover, because  $\zeta^k$  is bounded away from zero as  $k \rightarrow \infty$ , it must hold that

$$\lim_{k \rightarrow \infty} \tilde{\nabla} \tilde{\phi}(\mathbf{x}^k; \mathbf{x}^k) = \mathbf{0}. \tag{40}$$

Due to the compactness of  $\mathcal{D}$ , the sequence  $\{\mathbf{x}^k\}$  has at least one limit point, say  $\bar{\mathbf{x}}$ . Moreover, because  $\phi$  is continuously differentiable and the projection operation is a continuous mapping [30, Prop. B.11(c)], their composite  $\tilde{\nabla} \tilde{\phi}$  is a continuous mapping, which together with (40) implies

$$\tilde{\nabla} \tilde{\phi}(\bar{\mathbf{x}}; \bar{\mathbf{x}}) = \mathbf{0}.$$

On the other hand, notice that

$$\begin{aligned}
\tilde{\nabla} \tilde{\phi}(\bar{\mathbf{x}}; \bar{\mathbf{x}}) &= \mathcal{P}(\bar{\mathbf{x}} + \nabla \phi(\bar{\mathbf{x}})) - \bar{\mathbf{x}} \\
&= \mathcal{P}(\bar{\mathbf{x}} + \nabla \phi(\bar{\mathbf{x}})) - \bar{\mathbf{x}} \\
&= \tilde{\nabla} \phi(\bar{\mathbf{x}}; \bar{\mathbf{x}}),
\end{aligned}$$

where the second equality is due to the fact that  $\tilde{\phi}$  is a partial linearization of  $\phi$ . Therefore, we obtain  $\tilde{\nabla} \phi(\bar{\mathbf{x}}; \bar{\mathbf{x}}) = \mathbf{0}$ ; i.e.,  $\bar{\mathbf{x}}$  is a stationary point to problem (15).

#### F. Proof of Proposition 2

For ease of exposition, we prove only for the real variable case; extension to the complex domain is straightforward. Let us first consider the Armijo's stepsize rule; i.e.,  $\alpha^{k,l} = (\beta_{k,l})^{m_{k,l}}$  for some constant  $\beta_{k,l} \in (0, 1)$ , where the integer  $m_{k,l}$  is chosen as the smallest nonnegative integer such that the following inequality holds [30]

$$\begin{aligned}
& \tilde{\phi}(\mathbf{x}^{k,l} + (\beta_{k,l})^{m_{k,l}} \tilde{\nabla} \tilde{\phi}(\mathbf{x}^{k,l}; \mathbf{x}^k); \mathbf{x}^k) - \tilde{\phi}(\mathbf{x}^{k,l}; \mathbf{x}^k) \\
& \geq \sigma (\beta_{k,l})^{m_{k,l}} \left( \nabla \tilde{\phi}(\mathbf{x}^{k,l}; \mathbf{x}^k) \right)^T \tilde{\nabla} \tilde{\phi}(\mathbf{x}^{k,l}; \mathbf{x}^k),
\end{aligned} \tag{41}$$

for some constant  $\sigma \in (0, 1)$ . Next, we bound the right-hand side of (41) by using the following lemma [30, Prop. 2.1.3]:

**Lemma 3 (Projection Theorem)** *Let  $\mathcal{X}$  be a nonempty, closed and convex subset of  $\mathbb{R}^N$ . Given some  $\mathbf{x} \in \mathbb{R}^N$  and its projection  $\bar{\mathbf{x}}$  onto  $\mathcal{X}$ , i.e.,  $\bar{\mathbf{x}} = \mathcal{P}(\mathbf{x})$ , it holds that*

$$(\mathbf{x} - \bar{\mathbf{x}})^T (\mathbf{z} - \bar{\mathbf{x}}) \leq 0, \quad \forall \mathbf{z} \in \mathcal{X}.$$

Now, by substituting  $\mathbf{x} = \mathbf{x}^{k,l} + \nabla \tilde{\phi}(\mathbf{x}^{k,l}; \mathbf{x}^k)$  and  $\mathbf{z} = \mathbf{x}^{k,l}$  in Lemma 3 and denoting  $\bar{\mathbf{x}}^{k,l} = \mathcal{P}(\mathbf{x}^{k,l} + \nabla \tilde{\phi}(\mathbf{x}^{k,l}; \mathbf{x}^k))$ , we have

$$(\mathbf{x}^{k,l} + \nabla \tilde{\phi}(\mathbf{x}^{k,l}; \mathbf{x}^k) - \bar{\mathbf{x}}^{k,l})^T (\mathbf{x}^{k,l} - \bar{\mathbf{x}}^{k,l}) \leq 0.$$

Rearranging the above inequality yields

$$\nabla \tilde{\phi}(\mathbf{x}^{k,l}; \mathbf{x}^k)^T (\bar{\mathbf{x}}^{k,l} - \mathbf{x}^{k,l}) \geq \|\bar{\mathbf{x}}^{k,l} - \mathbf{x}^{k,l}\|^2,$$

i.e.,

$$\nabla \tilde{\phi}(\mathbf{x}^{k,l}; \mathbf{x}^k)^T \tilde{\nabla} \tilde{\phi}(\mathbf{x}^{k,l}; \mathbf{x}^k) \geq \|\tilde{\nabla} \tilde{\phi}(\mathbf{x}^{k,l}; \mathbf{x}^k)\|^2. \tag{42}$$

Combining Eqn. (41) and (42), we obtain

$$\begin{aligned}
& \tilde{\phi}(\mathbf{x}^{k,l} + (\beta_{k,l})^{m_{k,l}} \tilde{\nabla} \tilde{\phi}(\mathbf{x}^{k,l}; \mathbf{x}^k); \mathbf{x}^k) - \tilde{\phi}(\mathbf{x}^{k,l}; \mathbf{x}^k) \\
& \geq \sigma (\beta_{k,l})^{m_{k,l}} \|\tilde{\nabla} \tilde{\phi}(\mathbf{x}^{k,l}; \mathbf{x}^k)\|^2.
\end{aligned}$$

Recalling  $\mathbf{x}^{k,l+1} = \mathbf{x}^{k,l} + (\beta_{k,l})^{m_{k,l}} \tilde{\nabla} \tilde{\phi}(\mathbf{x}^{k,l}; \mathbf{x}^k)$  and taking summation over  $l$  from 0 to  $L_k - 1$  yields

$$\begin{aligned}
\tilde{\phi}(\mathbf{x}^{k+1}; \mathbf{x}^k) - \tilde{\phi}(\mathbf{x}^k; \mathbf{x}^k) &\geq \sigma \sum_{l=0}^{L_k-1} (\beta_{k,l})^{m_{k,l}} \|\tilde{\nabla} \tilde{\phi}(\mathbf{x}^{k,l}; \mathbf{x}^k)\|^2 \\
&\geq \underbrace{\sigma (\beta_{k,0})^{m_{k,0}}}_{\triangleq \zeta^k} \|\tilde{\nabla} \tilde{\phi}(\mathbf{x}^k; \mathbf{x}^k)\|^2.
\end{aligned}$$

Assuming for now that  $\sigma (\beta_{k,0})^{m_{k,0}}$  is bounded away from zero as  $k \rightarrow \infty$  (we will prove this shortly), we see that using Armijo's stepsize rule, the iteration fulfills the relation (22). Therefore, the convergence of Algorithm 1 follows directly from Proposition 1.

Now, we show that  $\sigma(\beta_{k,0})^{m_{k,0}}$  is indeed bounded away from zero as  $k \rightarrow \infty$ . The proof is inspired by Proposition 1.2.1 in [30]. Consider a convergent subsequence of  $\{\mathbf{x}^k\}$ , denoted by  $\{\mathbf{x}^k\}_{k \in \mathcal{K}}$ , with a limit point  $\bar{\mathbf{x}}$ , i.e.,  $\lim_{k \rightarrow \infty, k \in \mathcal{K}} \mathbf{x}^k = \bar{\mathbf{x}}$ . Suppose on the contrary that  $\limsup_{k \rightarrow \infty, k \in \mathcal{K}} \sigma(\beta_{k,0})^{m_{k,0}} = 0$ , i.e.,

$$\limsup_{k \rightarrow \infty, k \in \mathcal{K}} (\beta_{k,0})^{m_{k,0}} = 0.$$

Hence, by the definition of Armijo's rule, we must have for some index  $\bar{k}$  such that

$$\begin{aligned} & \tilde{\phi}\left(\mathbf{x}^{k,0} + \frac{(\beta_{k,0})^{m_{k,0}}}{\beta_{k,0}} \tilde{\nabla} \tilde{\phi}(\mathbf{x}^{k,0}; \mathbf{x}^k); \mathbf{x}^k\right) - \tilde{\phi}(\mathbf{x}^{k,0}; \mathbf{x}^k) \\ & < \sigma \frac{(\beta_{k,0})^{m_{k,0}}}{\beta_{k,0}} \left(\nabla \tilde{\phi}(\mathbf{x}^{k,0}; \mathbf{x}^k)\right)^T \tilde{\nabla} \tilde{\phi}(\mathbf{x}^{k,0}; \mathbf{x}^k), \end{aligned} \quad (43)$$

for all  $k \in \mathcal{K}$ ,  $k \geq \bar{k}$ . Denote  $\mathbf{p}^k = \tilde{\nabla} \tilde{\phi}(\mathbf{x}^{k,0}; \mathbf{x}^k) / \|\tilde{\nabla} \tilde{\phi}(\mathbf{x}^{k,0}; \mathbf{x}^k)\|$  and  $\bar{\alpha}^{k,0} = (\beta_{k,0})^{m_{k,0}} \|\tilde{\nabla} \tilde{\phi}(\mathbf{x}^{k,0}; \mathbf{x}^k)\| / \beta_{k,0}$ . Since  $\tilde{\phi}(\mathbf{x}; \mathbf{x}^k)$  is continuously differentiable and the feasible set  $\mathcal{D}$  is compact [cf. Eqn. (21)],  $\|\tilde{\nabla} \tilde{\phi}(\mathbf{x}^{k,0}; \mathbf{x}^k)\|$  is bounded, and thus

$$\limsup_{k \rightarrow \infty, k \in \mathcal{K}} \bar{\alpha}^{k,0} = 0.$$

In addition, since  $\|\mathbf{p}^k\| = 1$ , it has a limit point. By taking a further subsequence of  $\mathcal{K}$ , we can assume without loss of generality that  $\lim_{k \rightarrow \infty, k \in \mathcal{K}} \mathbf{p}^k = \bar{\mathbf{p}}$ . Now, by substituting  $\mathbf{p}^k$  and  $\bar{\alpha}^{k,0}$  into (43), we have

$$\frac{\tilde{\phi}(\mathbf{x}^{k,0} + \bar{\alpha}^{k,0} \mathbf{p}^k; \mathbf{x}^k) - \tilde{\phi}(\mathbf{x}^{k,0}; \mathbf{x}^k)}{\bar{\alpha}^{k,0}} < \sigma \nabla \tilde{\phi}(\mathbf{x}^{k,0}; \mathbf{x}^k)^T \mathbf{p}^k, \quad \forall k \in \mathcal{K}, k \geq \bar{k},$$

which further implies

$$\nabla \tilde{\phi}(\mathbf{x}^{k,0} + \bar{\alpha}^{k,0} \mathbf{p}^k; \mathbf{x}^k)^T \mathbf{p}^k < \sigma \nabla \tilde{\phi}(\mathbf{x}^{k,0}; \mathbf{x}^k)^T \mathbf{p}^k, \quad \forall k \in \mathcal{K}, k \geq \bar{k},$$

for some  $\bar{\alpha}^{k,0} \in [0, \bar{\alpha}^{k,0}]$  by applying the mean value theorem. Taking the limit and noticing  $\bar{\alpha}^{k,0} \rightarrow 0$  and  $\mathbf{x}^{k,0} = \mathbf{x}^k$ , we obtain

$$(1 - \sigma) \nabla \tilde{\phi}(\bar{\mathbf{x}}; \bar{\mathbf{x}})^T \bar{\mathbf{p}} \leq 0,$$

i.e.,

$$\nabla \tilde{\phi}(\bar{\mathbf{x}}; \bar{\mathbf{x}})^T \bar{\mathbf{p}} \leq 0. \quad (44)$$

On the other hand, it follows from (42) that

$$\nabla \tilde{\phi}(\mathbf{x}^{k,l}; \mathbf{x}^k)^T \frac{\tilde{\nabla} \tilde{\phi}(\mathbf{x}^{k,l}; \mathbf{x}^k)}{\|\tilde{\nabla} \tilde{\phi}(\mathbf{x}^{k,l}; \mathbf{x}^k)\|} \geq \|\tilde{\nabla} \tilde{\phi}(\mathbf{x}^{k,l}; \mathbf{x}^k)\|.$$

By setting  $l = 0$  and taking limit over  $k \in \mathcal{K}$ , we get

$$\nabla \tilde{\phi}(\bar{\mathbf{x}}; \bar{\mathbf{x}})^T \bar{\mathbf{p}} \geq \|\tilde{\nabla} \tilde{\phi}(\bar{\mathbf{x}}; \bar{\mathbf{x}})\|.$$

Let us consider two possibilities for the limit point  $\bar{\mathbf{x}}$ : 1) if  $\bar{\mathbf{x}}$  is a stationary point, then there is nothing to prove and Proposition 2 holds trivially; 2) if  $\bar{\mathbf{x}}$  is not a stationary point, then we must have

$$\|\tilde{\nabla} \tilde{\phi}(\bar{\mathbf{x}}; \bar{\mathbf{x}})\| > 0.$$

Hence,  $\nabla \tilde{\phi}(\bar{\mathbf{x}}; \bar{\mathbf{x}})^T \bar{\mathbf{p}} > 0$ , but this contradicts with (44). Therefore,  $\sigma(\beta_{k,0})^{m_{k,0}}$  is bounded away from zero.

For the (limited) minimization stepsize rule, the proof is essentially the same as that of Armijo's stepsize rule if one notice that

$$\begin{aligned} & \tilde{\phi}\left(\mathbf{x}^{k,l} + \eta^{k,l} \tilde{\nabla} \tilde{\phi}(\mathbf{x}^{k,l}; \mathbf{x}^k); \mathbf{x}^k\right) - \tilde{\phi}(\mathbf{x}^{k,l}; \mathbf{x}^k) \\ & \geq \tilde{\phi}\left(\mathbf{x}^{k,l} + (\beta_{k,l})^{m_{k,l}} \tilde{\nabla} \tilde{\phi}(\mathbf{x}^{k,l}; \mathbf{x}^k); \mathbf{x}^k\right) - \tilde{\phi}(\mathbf{x}^{k,l}; \mathbf{x}^k) \\ & \geq \sigma(\beta_{k,l})^{m_{k,l}} \left(\nabla \tilde{\phi}(\mathbf{x}^{k,l}; \mathbf{x}^k)\right)^T \tilde{\nabla} \tilde{\phi}(\mathbf{x}^{k,l}; \mathbf{x}^k), \end{aligned}$$

where  $\eta^{k,l} > 0$  is the stepsize obtained from (limited) minimization rule. Consequently, the proof for (limited) minimization rule boils down to that of Armijo's stepsize rule.

### G. Proof of Theorem 3

The proof is basically the same as that of Theorem 1. Here, we just give a sketched proof. It is easy to verify that Lemma 1 still holds if we add the power transfer constraint (28c) in problems (17) and (18). Moreover, notice that there are in total 8 constraints in (28); hence it follows from the rank-reduction result [28, Lemma 3.1] that there exists an optimal  $(\mathbf{W}^*, \mathbf{Q}^*)$  for problem (28) fulfilling

$$\text{rank}(\mathbf{W}^*) \leq \sqrt{8} < 3.$$

That is,  $\text{rank}(\mathbf{W}^*) \leq 2$ . The remaining proof is exactly the same as that of Theorem 1 and thus omitted.

### REFERENCES

- [1] D. Kim, H. Lee, and D. Hong, "A survey of in-band full-duplex transmission: From the perspective of PHY and MAC layers," *IEEE Commun. Survey and Tutorials*, vol. 17, no. 4, pp. 2017–2046, Feb. 2015.
- [2] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Trans. Signal Process.*, vol. 61, no. 20, pp. 4962–4974, Oct. 2013.
- [3] L. Li, Z. Chen, D. Zhang, and J. Fang, "A full-duplex Bob in the MIMO Gaussian wiretap channel: Scheme and performance," *IEEE Sig. Process. Lett.*, vol. 23, no. 1, pp. 107–111, Jan. 2016.
- [4] R. Feng, Q. Li, Q. Zhang, and J. Qin, "Robust secure beamforming in MISO full-duplex two-way secure communications," *IEEE Trans. veh. Tech.*, vol. 65, no. 1, pp. 408–414, Jan. 2016.
- [5] Y. Wang, Q. Li, Q. Zhang, and J. Qin, "Optimal and suboptimal full-duplex secure beamforming designs for MISO two-way communications," *IEEE Wireless Commun. Lett.*, vol. 4, no. 5, pp. 493–496, Oct. 2015.
- [6] F. Zhu, F. Gao, M. Yao, and H. Zou, "Joint information- and jamming-beamforming for physical layer security with full duplex base station," *IEEE Trans. Sig. Process.*, vol. 62, no. 24, pp. 6391–6401, Dec. 2014.
- [7] Y. Sun, D. W. K. Ng, J. Zhu, and R. Schober, "Multi-objective optimization for robust power efficient and secure full-duplex wireless communication systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 8, pp. 5511–5526, Aug. 2016.
- [8] S. Parsaeeefard and T. Le-Ngoc, "Improving wireless secrecy rate via full-duplex relay-assisted protocols," *IEEE Trans. Info. Forensics Security*, vol. 10, no. 10, pp. 2095–2107, Oct. 2015.
- [9] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Physical layer network security in the full-duplex relay system," *IEEE Trans. Info. Forensics Security*, vol. 10, no. 3, pp. 574–583, Mar. 2015.
- [10] J. Lee, "Full-duplex relay for enhancing physical layer security in multi-hop relaying systems," *IEEE Commun. Lett.*, vol. 19, no. 4, pp. 525–528, Apr. 2015.
- [11] X. Kang, C. K. Ho, and S. Sun, "Full-duplex wireless-powered communication network with energy causality," *IEEE Trans. Wireless Commun.*, vol. 14, no. 10, pp. 5539–5551, Oct. 2015.



- [12] H. Ju and R. Zhang, "Optimal resource allocation in full-duplex wireless powered communication network," *IEEE Trans. Commun.*, vol. 62, no. 10, pp. 3528–3540, Oct. 2014.
- [13] C. Zhong, H. A. Suraweera, G. Zheng, I. Krikidis, and Z. Zhang, "Wireless information and power transfer with full duplex relaying," *IEEE Trans. Commun.*, vol. 62, no. 10, pp. 3447–3461, Oct. 2014.
- [14] Y. Zeng and R. Zhang, "Full-duplex wireless-powered relay with self-energy recycling," *IEEE Wireless Commun. Lett.*, vol. 4, no. 2, pp. 201–204, Apr. 2015.
- [15] I. Krikidis, S. Timotheou, S. Nikolaou, G. Zheng, D. W. K. Ng, and R. Schober, "Simultaneous wireless information and power transfer in modern communication systems," *IEEE Commun. Mag.*, vol. 52, no. 11, pp. 104–110, Nov. 2014.
- [16] J.-H. Lee, "Full-duplex relay for enhancing physical layer security in multi-hop relaying systems," *IEEE Commun. Lett.*, vol. 19, no. 4, pp. 525–528, Apr. 2015.
- [17] S. Parsaefard and T. Le-Ngoc, "Improving wireless secrecy rate via full-duplex relay-assisted protocols," *IEEE Trans. Info. Forensics Security*, vol. 10, no. 10, pp. 2095–2107, Oct. 2015.
- [18] X. Wu, W.-K. Ma, and A. M.-C. So, "Physical-layer multicasting by stochastic transmit beamforming and Alamouti space-time coding," *IEEE Trans. Sig. Process.*, vol. 61, no. 17, pp. 4230–4245, Sept. 2013.
- [19] D. R. Hunter and K. Lange, "A tutorial on MM algorithms," *The American Statistician*, vol. 58, no. 12, pp. 30–37, 2004.
- [20] G. Zheng, "Joint beamforming optimization and power control for full-duplex MIMO two-way relay channel," *IEEE Trans. Sig. Process.*, vol. 63, no. 3, pp. 555–566, Feb. 2015.
- [21] Q. Li and D. Han, "Sum secrecy rate maximization for full-duplex two-way relay networks," in *Proc. ICASSP 2016*, Mar. 2016, pp. 3641–3645.
- [22] R. Zhang, Y. C. Liang, C. C. Chai, and S. Cui, "Optimal beamforming for two-way multi-antenna relay channel with analogue network coding," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 5, pp. 699–712, Jun. 2009.
- [23] S. Alamouti, "A simple transmitter diversity scheme for wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 16, no. 8, pp. 1451–1458, Jun. 1998.
- [24] E. Tekin and A. Yener, "The general Gaussian multiple access and two-way wire-tap channels: Achievable rates and cooperative jamming," *IEEE Trans. Infor. Theory*, vol. 54, no. 3, pp. 2735–2751, Jun. 2008.
- [25] Z.-Q. Luo, W.-K. Ma, A. M.-C. So, Y. Ye, and S. Zhang, "Semidefinite relaxation of quadratic optimization problems," *IEEE Signal Process. Mag.*, vol. 27, no. 3, pp. 20–34, May 2010.
- [26] M. Grant and S. Boyd, "CVX: Matlab software for disciplined convex programming, version 2.1," <http://cvxr.com/cvx>, Mar. 2014.
- [27] M. Razaviyayn, M. Hong, and Z.-Q. Luo, "A unified convergence analysis of block successive minimization methods for nonsmooth optimization," *SIAM J. Opt.*, vol. 23, no. 2, pp. 1126–1153, 2013.
- [28] Y. Huang and D. P. Palomar, "Rank-constrained separable semidefinite programming with applications to optimal beamforming," *IEEE Trans. Signal Process.*, vol. 58, no. 2, pp. 664–678, 2010.
- [29] Y. Nesterov, *Introductory lectures on convex optimization: A basic course*. Kluwer Academic Publisher, 2004.
- [30] D. Bertsekas, *Nonlinear Programming*. Belmont, MA: Athena Scientific, 1999.
- [31] Q. Li, M. Hong, H.-T. Wai, Y.-F. Liu, W.-K. Ma, and Z.-Q. Luo, "Transmit solutions for MIMO wiretap channels using alternating optimization," *IEEE Journal Sel. Area. Commun.*, vol. 31, no. 9, pp. 1714–1727, Nov. 2013.